Reference Guide

VMware vCenter Server Heartbeat 5.5 Update 2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000206-01

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 7

Getting Started

1 Introduction 11
- vCenter Server Heartbeat Concepts 11
  - Server Protection 12
  - Network Protection 12
  - Application Protection 12
  - Performance Protection 13
  - Data Protection 14
  - Communications 14
- Switchover Process 15
  - Auto Switchovers 16
- Failover Process 17
  - Recovery from a Failover 17

Installation

2 vCenter Server Heartbeat Implementation 21
- Overview 21
- Environmental Prerequisites 21
- Common Requirements 22
- Server Architecture Options 22
  - Virtual to Virtual (V2V) 22
  - Physical to Virtual (P2V) 23
  - Physical to Physical (P2P) 23
- Cloning Technology Options 24
  - Supported Pre-Clone Technologies 24
  - Supported Install Clone Technologies 24
- Application Component Options 25
  - vCenter Server with SQL Server on the Same Host 25
  - vCenter Server with SQL Server on a Separate Host 25
  - vCenter Server Only 25
- Network Options 25
  - LAN 26
  - WAN 26
- Antivirus Recommendations 27
- Deployment Options Summary 28
- Installation Options Checklist 28

3 vCenter Server Heartbeat Installation on Windows Server 2003 31
- Overview 31
- Installation Process 31
- Primary Server 32

Secondary Server 53
Post Installation Configuration 68
Add the VMware License 68
When Deployed in a WAN Environment 68
vCenter Server 2.5 68
vCenter Server 4.0 69

4 vCenter Server Heartbeat Installation on Windows Server 2008 71
Overview 71
Installation Process 71
Primary Server 72
Secondary Server 92
Post Installation Configuration 109
Add the VMware License 109
When Deployed in a WAN Environment 109
vCenter Server 2.5 109
vCenter Server 4.0 110

5 Configuring vCenter Server Heartbeat 113
Server Configuration Wizard 114
Configuring the Machine Identity 115
Configuring the Server Role 115
Configuring the Client Connection Port 115
Configuring Channel IP Routing 115
Configuring the Default Channel Port 116
Configuring Low Bandwidth Module 116
Configuring Public IP Addressing 116
Enabling Network Monitoring 117
Configuring Split-Brain Avoidance 118
Managing vCenter Server Heartbeat License Keys 119
Configuring Message Queue Logs 119
Configuring the Maximum Disk Usage 120

System Administration and Management

6 Server Protection 123
Server Protection Overview 123
Checking the Server Pair Status 124
Configuring Heartbeat Settings 125
Configuring vCenter Server Heartbeat Shutdown Options 126
Starting, Stopping, and Shutting Down vCenter Server Heartbeat 126
Forcing a Switchover 127
Recovering From a Failover 128
Configuring Split-Brain Avoidance 129

7 Network Protection 131
Communication Status 131
Reviewing the VMware Channel Status 131
Configuring Public Network Connection Checks 132
Setting Max Server Time Difference 133

8 Application Protection 135
Application Protection Overview 135
Applications Tab 135
Editing Individual Applications 136
Configuring Applications 137
Reviewing the Status of an Application 138
Reviewing the Application Log 138
Filtering Application Log Entries 139
Resetting the Application Health Status 140
Removing an Application 140
Services Tab 141
Adding a Service 142
Editing a Service 143
Checking the Status of Services 144
Unprotecting Services and Stopping Monitoring 144
Removing a Service 145
Tasks Tab 146
Adding a Task 146
Editing a Task 147
Removing a Task 148
Starting a Task Manually 148
Plugins Tab 149
Installing a Plug-In 150
Editing a Plug-in 151
Uninstalling a Plug-in 152

9 Status and Control 153
vCenter Server Heartbeat Console 153
Logging into vCenter Server Heartbeat 153
Connecting to a Pair of Servers 155
Reviewing the Status of a Server Pair 155
Configuring the Look and Feel of the vCenter Server Heartbeat Console 156
Changing vCenter Server Heartbeat Console Pages 157
Logging Out of the vCenter Server Heartbeat Console 157

10 Performance Protection 159
Rules Tab 159
Editing a Rule 160
Rules Installed by vCenter Server Heartbeat Plug-Ins 160
Checking a Rule Condition 162

11 Data Protection 163
Data Protection Overview 164
Automatic Filter Discovery 164
Adding a User-Defined Inclusion Filter 165
Adding a User-Defined Exclusion Filter 166
Removing User-Defined Inclusion or Exclusion Filters 167
Configuring Max Disk Usage 167
Reviewing Status of Protected Files 168
Determining Effective Filters 168
Initiating File Synchronization Manually 169
Initiating Verify and Synchronize Manually 170
Initiating a Full System Check 170
Reviewing the Registry Synchronization Status 171

Initiating a Full Registry Check 172

12 Other Administrative Tasks 173
Configuring Alerts 173
Configuring Alert Reporting 174
Test Alert Reporting 176
Configuring Event Log Files 177
Configuring Log File Email Recipients 177
Reviewing Event Logs 178

13 Troubleshooting 181
Troubleshooting Unexpected Behaviors 181
Two Active Servers 181
Symptoms 181
Causes 182
Resolution 182
Two Passive Servers 183
Symptom 183
Causes 183
Resolution 183
Synchronization Failures 184
Services Running on the Passive Server 184
VMware Channel Incorrectly Configured 184
Incorrect or Mismatched Disk Configuration 185
Passive Server Has Less Available Space than Active Server 185
Registry Status is Out of Sync 186
Resource Issues 186
Registry Security Issues 186
Channel Drops 186
Performance Issues 186
Passive Server Does Not Meet Minimum Hardware Requirements 187
Hardware or Driver Issues on VMware Channel NICs 187
Firewall Connection 188
Incorrect VMware Channel Configuration 188
VMware vCenter Server Heartbeat Packet Filter Is Enabled on the Channel NIC(s) 189
Subnet or Routing Issues 190
LAN Deployment 190
WAN Deployment 190
MaxDiskUsage Errors 190
Active Server (Unsafe) Queue 191
Passive Server (Safe) Queue 191
MaxDiskUsage Error Messages 191
[L9]Exceeded the Maximum Disk Usage (VCChannelExceededMaxDiskUsageException) 191
[L9]Exceeded the Maximum Disk Usage on the ACTIVE Server 191
[L9]Exceeded the Maximum Disk Usage on the PASSIVE Server 192
[L20]Out of Disk Space (VCChannelOutOfDiskSpaceException) 193
Application Slowdown 193
Poor Application Performance 193
Both Servers Can Accommodate the Initial Load but the Load Has Increased 194
One Server Can Provide Adequate Resource Support, but the Other Cannot 194
Scheduled Resource Intensive Tasks 195

Appendix – Setup Error Messages 197

Glossary 199

About This Book

The *Reference Guide* provides information about installing and configuring VMware vCenter Server Heartbeat, including implementation in a Local Area Network (LAN) or Wide Area Network (WAN), configuring network protection, application protection, data protection, Split-brain Avoidance, and more. To help you protect your VMware vCenter Server, the book provides an overview of protection offered by vCenter Server Heartbeat and the actions that vCenter Server Heartbeat can take in the event of a network, hardware, or application failure.

Intended Audience

This guide assumes a working knowledge of networks including configuration of TCP/IP suite of protocols and sound knowledge of domain administration on the Windows 2003 platform, notably in Active Directory and DNS.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Abbreviations Used in Figures

The figures in this book use the abbreviations listed in Table 1.

Table 1. Abbreviations

Abbreviation	Description
Channel	VMware Channel
NIC	Network interface card
P2P	Physical to physical
P2V	Physical to virtual
V2V	Virtual to virtual
SAN	Storage area network type datastore

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to www.vmware.com/support/phone_support.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands on labs, case study examples, and course materials designed for use as on the job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to www.vmware.com/services.

Getting Started

Introduction 1

This chapter includes the following topics:

- "vCenter Server Heartbeat Concepts" on page 11
- "Switchover Process" on page 15
- "Failover Process" on page 17

vCenter Server Heartbeat Concepts

vCenter Server Heartbeat is a Windows based service specifically designed to provide high availability protection for vCenter Server configurations without requiring any specialized hardware.

vCenter Server Heartbeat provides the following protection levels:

- **Server Protection** – vCenter Server Heartbeat provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, vCenter Server Heartbeat protects the network identity of the production server, ensuring users are provided with a replica server including server name and IP address shares on the failure of the production server.
- **Network Protection** – vCenter Server Heartbeat proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network.
- **Application Protection** – vCenter Server Heartbeat maintains the application environment ensuring that applications and services stay alive on the network.
- **Performance Protection** – vCenter Server Heartbeat proactively monitors system performance attributes to ensure that the system administrator is notified of problems and can take pre-emptive action to prevent an outage.
- **Data Protection** – vCenter Server Heartbeat intercepts all data written by users and applications, and maintains a copy of this data on the passive server that can be used in the event of a failure.

vCenter Server Heartbeat provides all five protection levels continuously, ensuring all facets of the user environment are maintained at all times, and that the network (Principal (Public) network) continues to operate through as many failure scenarios as possible.

vCenter Server Heartbeat software is installed on a Primary server and a Secondary server. These names refer to the physical hardware (identity) of the servers.

The Secondary server has the same domain name, same file and data structure, same network address, and can run all the same applications and services as the Primary server.

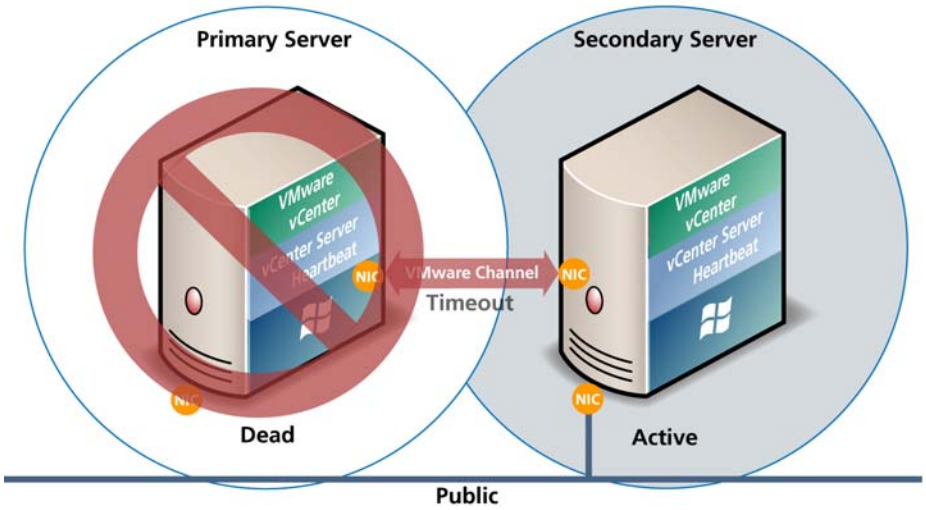
vCenter Server Heartbeat uses two servers with identical names and IP addresses. One is an active server that is visible on the Principal (Public) network and the other is a passive server that is hidden from the network but remains as a ready standby server. Only one server name and IP address can be visible on the Principal (Public) network at any given time.

The vCenter Server Heartbeat software is symmetrical in almost all respects, and either the Primary Server or the Secondary server can take the active role and provide the protected application to the user.

Server Protection

vCenter Server Heartbeat maintains availability through operating system and hardware failure events. Two instances of vCenter Server Heartbeat monitor each other by sending "I'm alive" messages and reciprocating with acknowledgments over a network connection termed the VMware Channel. If the passive server detects that this process or heartbeat has failed, a failover is initiated as illustrated in Figure 1-1.

Figure 1-1. Failover



A failover is similar to a switchover but is used in more drastic situations. A failover happens when the passive server detects that the active server is no longer responding. This can occur when the active server hardware crashes or loses its network connections. Rather than the active server gracefully closing, the passive server determines that the active server has failed and requires no further operations. During failover, the passive server immediately takes on the active server role. The mechanics of failovers are discussed later in this guide.

Network Protection

vCenter Server Heartbeat proactively monitors the capability of the active server to communicate with the rest of the network by polling defined nodes around the network, including by default the default gateway, the primary DNS server, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, due to a network card failure or a local switch failure, vCenter Server Heartbeat can initiate a switchover, allowing the Secondary server to assume an identical network identity as the Primary server.

Application Protection

vCenter Server Heartbeat running locally on the active server monitors the protected applications and services through the use of plug-ins. vCenter Server Heartbeat protects the following components:

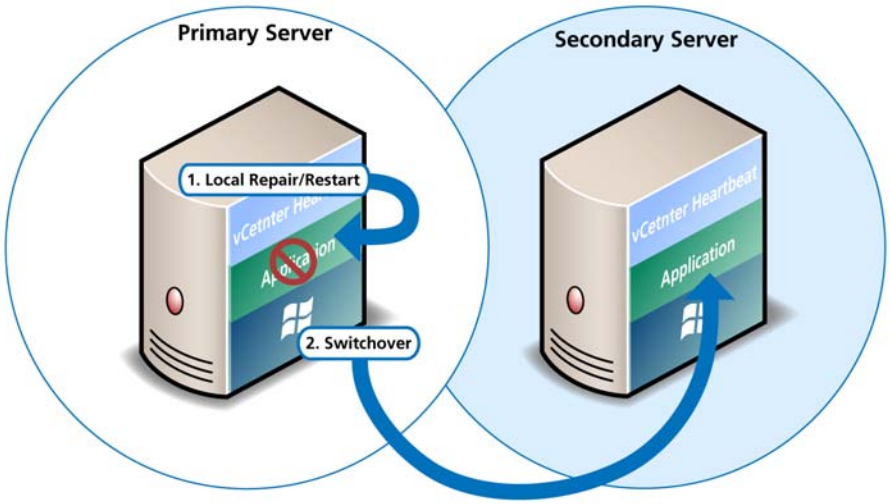
- VirtualCenter Server Versions 2.5
  - VMware VirtualCenter Server
  - VMware Capacity Planner
  - VMware Converter Enterprise
  - VMware Update Manager
  - VMware License Server
- vCenter Server Version 4.0
  - VMware vCenter Server
  - VMware Guided Consolidation Service

- VMware License Sever
- VMware ADAM
- VMware vCenter Management Web Server
- VMware Update Manager
- VMware Converter Enterprise
- Guided Consolidation Service
- VMware Orchestrator
- VMware vSphere Host Update Utility

If a protected application fails, vCenter Server Heartbeat first tries to restart the application on the active server (1) in Figure 1-2.

If the application does not successfully restart, vCenter Server Heartbeat initiates a switchover (2) in Figure 1-2. Refer to "Switchover Process" on page 15 and "Failover Process" on page 17 for further information about the switchover process.

Figure 1-2. Switchover



A switchover gracefully closes any protected applications that are running on the active server and restarts them on the passive server, including the application or service that caused the failure. In the example where the Primary server is active and the Secondary server is passive, the Primary server is demoted to a passive role and is hidden from the network when the Secondary server is promoted to an active role and is made visible to the network. The mechanics of switchovers are discussed in more detail later in this guide.

Performance Protection

Ensuring that your protected applications are operational and providing service at a level of performance adequate for users to remain productive is important. The vCenter Server Heartbeat plug-in provides these monitoring and pre-emptive repair capabilities.

vCenter Server Heartbeat monitors application services and specific application attributes to ensure that protected applications are operational and not in an unresponsive or stopped state. This level of monitoring is fundamental in ensuring that applications are available to end users.

In addition to monitoring application services, vCenter Server Heartbeat can also monitor specific application attributes to ensure that they remain within normal operating ranges. Similar to application monitoring, various rules can trigger specific corrective actions whenever these attributes fall outside of their respective ranges.

Furthermore, vCenter Server Heartbeat provides the same level of flexibility to define and perform multiple corrective actions in the event of problems on a service by service or even attribute by attribute basis.

Data Protection

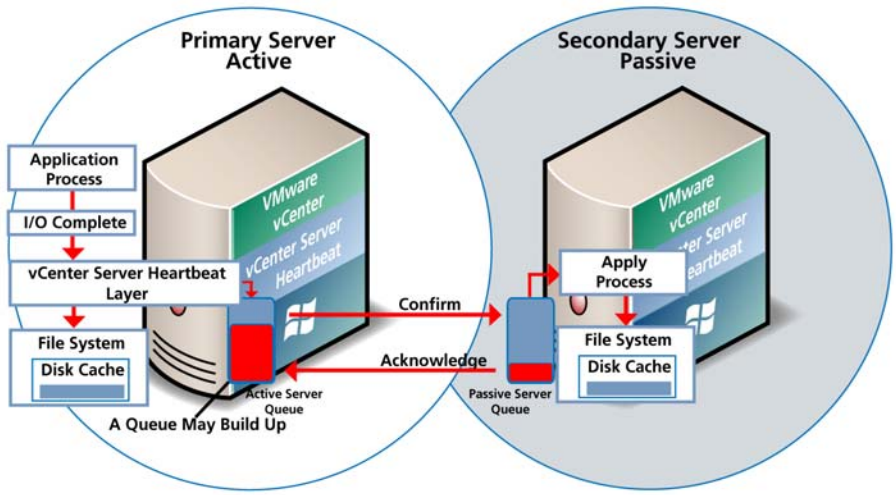
You can configure vCenter Server Heartbeat to protect the application environment. All data files that users or the applications require in the application environment are made available should a failure occur. After installation, vCenter Server Heartbeat configures itself to protect files, folders, and registry settings for vCenter Server on the active server by mirroring them in real time to the passive server. This means that if a failover occurs, all the files that were protected on the failed server are available to users after the failover, hosted on the Secondary server.

vCenter Server Heartbeat intercepts all file system I/O operations on the active server. If the intercepted write and update operations are within the protected set, these are placed in a queue on the active server referred to as the active server (unsafe) queue, pending transmission to the passive server. Each request is numbered to maintain its order in the queue.

With the request in the active server (unsafe) queue, vCenter Server Heartbeat allows the disk I/O to continue with the requested disk operation.

If the channel is connected, the active server (unsafe) queue is transferred to the passive server, which places all the requests in the passive server (safe) queue. The passive server confirms the changes were logged by sending the active server an acknowledgement. The active server clears the data from its queue.

Figure 1-3. Apply Process



The apply process running on the passive server (safe) queue applies all updates in strict sequence, duplicating an identical set of file operations on the passive server as illustrated in Figure 1-3.

Communications

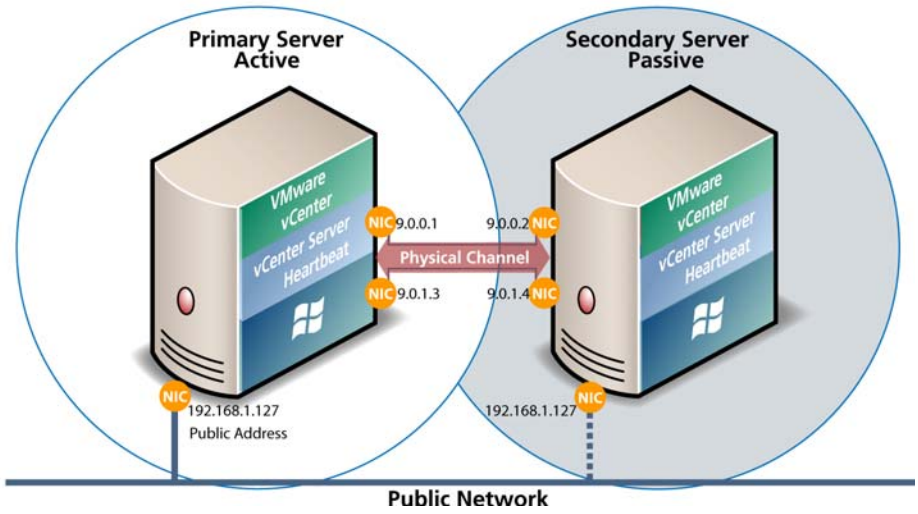
The VMware Channel is a crucial component of the setup and can be configured in a number of ways.

Both the Primary and Secondary servers must have two or more network interface connections (NICs).

The Principal (Public) network requires one NIC. The VMware Channel uses a separate NIC for the private connection between the servers used for control and data transfer between the pair of servers.

A second pair of NICs can be used to provide a degree of redundancy for the VMware Channel. In this configuration, the VMware Channel has a dual channel if more than one dedicated NIC is provided for the VMware Channel on each server. To provide added resilience, the communications for the second channel must be completely independent from the first channel. They must not share any switches, virtual switches, routers or the same WAN connection.

Figure 1-4. Communication Between Primary and Secondary Servers



The IP address used by a client to connect to the active server (the Principal (Public) IP address) must be configured to use a static IP address that is not DHCP (Dynamic Host Configuration Protocol) enabled. In the example in Figure 1-4, the IP address is configured as 192.168.1.127.

NOTE Obtain the IP address: type **`ipconfig`** at the prompt in a DOS shell. For additional information about the IP configuration, type **`/All`**.

The Principal (Public) NICs on the passive server are configured to use the same IP address as that of the active server but are prevented from communicating with the live network through an IP packet filtering system installed with vCenter Server Heartbeat. This packet filter prevents traffic using the Principal (Public) address from being committed to the wire. It also prevents NetBIOS traffic utilizing other IP addresses on the NIC from being sent to prevent NetBIOS name resolution conflicts.

The NICs on the active and passive servers used for the VMware Channel must be configured so that they have IP addresses outside of the Principal (Public) networks subnet range. These addresses are termed the VMware Channel addresses.

During installation, setup will switch off NetBIOS for the VMware Channel(s) on the active and passive servers as this connection remains live and both the passive and active machines have the same NetBIOS name. After restore and after the vCenter Server Heartbeat installation is complete (runtime), NetBIOS is disabled across the channel(s).

The NICs that allow the connectivity across the VMware Channel can be standard 100BaseT Ethernet cards providing a throughput of 100 Mbits per second across standard Cat-5 cabling. In its most basic form, a dedicated channel requires no hubs or routers, but the direct connection requires crossover cabling.

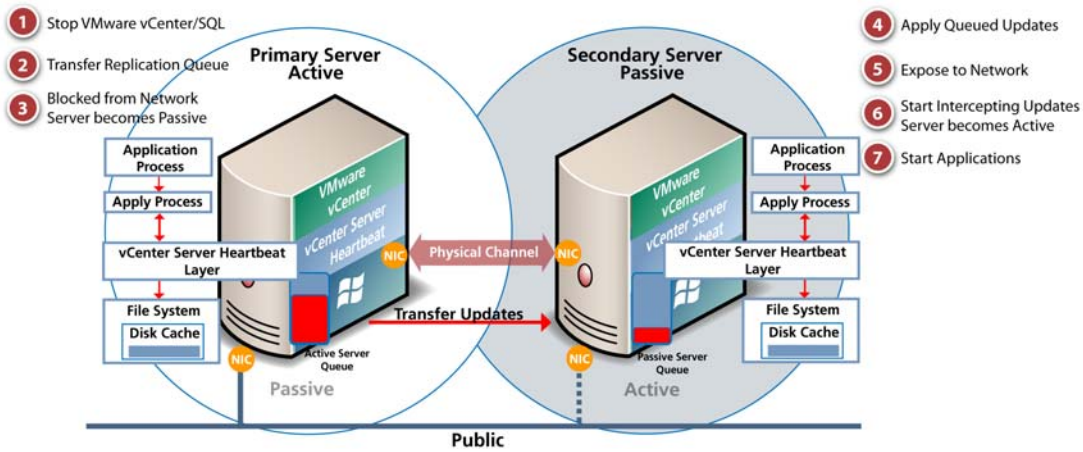
When configured for a WAN deployment, configure the VMware Channel to use static routes over switches and routers to maintain continuous communications independent from corporate or public traffic.

Switchover Process

You can trigger a switchover manually from **vCenter Server Heartbeat Console Status & Control** window by clicking **Switchover.** vCenter Server Heartbeat can initiate a switchover when a protected application fails or suffers performance degradation, or a network failure prevents the active server from being visible to the network.

When a switchover is triggered, the running of protected applications is transferred from the active machine to the passive machine in the server pair. The server roles are switched.

Figure 1-5. Switchover



The automatic procedure executed during a switchover operation involves the following steps:

1 Stop the protected applications on the active server. After the protected applications stop, no more disk updates are generated.

2 Send all updates that are still queued on the active server to the passive server. After this step, all updates are available on the passive server.

3 Change the status of the active server to switching to passive. The server is now no longer visible from the network.

4 Apply all queued updates on the passive server.

5 Change the status of the passive server to active. The new active server starts intercepting disk I/Os and queues them for the new passive server. The new active server is now visible on the network with the same identity as the old active server.

6 Change the status of the old active server from switching to passive to passive. The new passive server now accepts updates from the active server.

7 Start the same protected applications on the new active server. The protected applications now start and are accessible to users, generating disk updates.

The switchover is complete.

Auto Switchovers

An auto switchover is triggered when a protected application or other system monitored component such as networking fails.

An auto switchover is different than a manual switchover. Although the server roles are changed, replication stops so the administrator can investigate and rectify the cause of the auto switchover.

Auto switchover is similar to failover but caused by a failed monitored application or system component. After you determine the cause for the auto switchover, restore the server with the failed application or other system monitored component to the active role as follows:

1 Correct the incident that caused the failover.

2 Verify the integrity of the disk data on the failed server.

3 Restart the failed server.

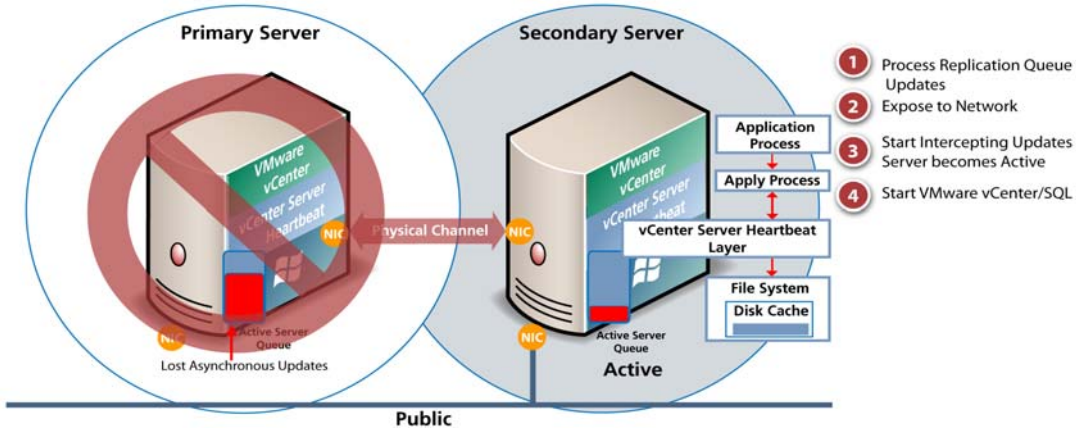
4 Start vCenter Server Heartbeat on the failed server.

5 Wait until vCenter Server Heartbeat is fully synchronized.

6 Perform a manual switchover.

Failover Process

Figure 1-6. Failover



When the passive server detects the active server is no longer running properly, it assumes the active server role by taking the following steps.

1 The server applies any intercepted updates that are currently saved in the passive server (safe) update queue, that is, the log of update records saved on the passive server but not yet applied to the replicated files.

   The length of the passive server (safe) queue affects the time the failover process takes to complete. If the passive server queue is long, the system must wait for application of all passive server updates before the rest of the process can take place.

   When no more update records can be applied, any update records that the server was unable to apply are discarded. An update record can only be applied if all earlier update records were applied and the completion status for the update is in the passive server (safe) update queue.

2 The server switches its role from passive to active.

   The server enables the public identity of the server. The active and passive servers both have the same system name and same Principal (Public) IP address. This Principal (Public) IP address can be enabled on only one of the two systems at a time. When the public identity is enabled, any clients connected to the server before the failover can now reconnect.

3 The server starts intercepting updates to the protected data. Updates to the protected data are saved in the active server (unsafe) update queue.

4 The server starts all the protected applications. The applications use the replicated application data to recover before allowing clients to reconnect. Any updates that the applications make to the protected data are intercepted and logged.

At this stage, the originally active server is offline, and the originally passive server has taken over the active server role and is running the protected applications. Because the originally active server stopped abruptly, the protected applications possibly lost some data, but the no synchronization mode update that completed before the failover is lost. The application clients can reconnect to the application and continue running as before.

During a failover, the data in the active server (unsafe) queue is lost.

Recovery from a Failover

Assuming that the active server before the failover was the Primary server, and the Secondary server has assumed the active role following a failover, you can reinstate the Primary server to an active role after rectifying the problem that initiated the failover.

When vCenter Server Heartbeat starts on the failed Primary server, it detects that it did not stop cleanly the previous time. It disables the public identity by deploying the IP packet filter at startup, and halts vCenter Server Heartbeat so that the issues that caused the failure can be resolved. The following steps restore the previously failed server to the active role:

1 Correct the incident that caused the failover.

2 Verify the integrity of the disk data on the failed server.

3 Restart the failed server.

4 Start vCenter Server Heartbeat on the failed server.

5 Wait until vCenter Server Heartbeat is fully synchronized.

6 Perform a manual switchover.

After resolving these issues, you can start vCenter Server Heartbeat on the failed, now passive, server. At this stage, the vCenter Server Heartbeat software running on the pair of servers connects and starts to synchronize the data on the Primary server. When the resynchronization is complete, you can continue operating with this configuration (for example, the Secondary server is the active server and the Primary server is the passive server), or perform a switchover to reverse the roles of the two servers in the vCenter Server Heartbeat pair (for example, assigning the Primary and Secondary the same roles that they had before the failover).

Installation

vCenter Server Heartbeat Implementation 2

This chapter includes the following topics:

- "Overview" on page 21
- "Environmental Prerequisites" on page 21
- "Common Requirements" on page 22
- "Server Architecture Options" on page 22
- "Cloning Technology Options" on page 24
- "Application Component Options" on page 25
- "Network Options" on page 25
- "Antivirus Recommendations" on page 27
- "Deployment Options Summary" on page 28

Overview

vCenter Server Heartbeat is a versatile solution that provides you with complete protection of vCenter Server and SQL Server. It can be deployed in a LAN for high availability or across a WAN to provide disaster recovery. vCenter Server Heartbeat can protect vCenter Server and SQL Server installed on the same server, or protect vCenter Server and SQL Server on separate servers. This flexibility enables vCenter Server Heartbeat to protect vCenter Server when using remote databases other than SQL Server.

This chapter discusses the deployment options and prerequisites necessary to successfully implement vCenter Server Heartbeat and provides a step by step process to assist in selecting options required for installation. The deployment scenario table provides a visual reference to configuration options supported by vCenter Server Heartbeat.

During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. A critical stop or warning message appears if the server fails a check. Refer to the Appendix – Setup Error Messages in this guide for a list of the checks and an explanation of the message. You must resolve critical stops before you can proceed with setup.

Prior to installing vCenter Server Heartbeat, select the deployment options you intend to use. The installation process prompts you to select options throughout the procedure to create the configuration you want.

Environmental Prerequisites

vCenter Server Heartbeat cannot protect a server configured with the following roles: domain controller, global catalog, or DNS. Please note, because vCenter Server Heartbeat only protects the vCenter Server and SQL Server applications, no other critical business applications should be installed on the server.

Common Requirements

The following requirements are in addition to those required for vCenter Server and SQL Server.

- Supported vCenter Server Versions
  - VirtualCenter Server 2.5
  - VirtualCenter Server 2.5 Update 1
  - VirtualCenter Server 2.5 Update 2
  - VirtualCenter Server 2.5 Update 3
  - VirtualCenter Server 2.5 Update 4
  - VirtualCenter Server 2.5 Update 5
  - vCenter Server 4.0
  - vCenter Server 4.0 Update 1
- Operating System
  - Windows Server 2003 x86 SP1 or SP2
  - Windows Server 2003 x64 SP2
  - Windows Server 2008 x86 SP1 or SP2
  - Windows Server 2008 x64 SP1 or SP2
- Prior to installing vCenter Server Heartbeat, verify that vCenter Guided Consolidation, vCenter Update Manager, and vCenter Converter are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses.
- During the setup process, vCenter Server Heartbeat verifies that a minimum of 1GB RAM is available. To ensure proper operation, vCenter Server Heartbeat requires a minimum of 1GB RAM (2GB is recommended) in addition to any other memory requirement for the Operating System or vCenter Server.
- Verify that 2GB of disk space is available on the installation drive for vCenter Server Heartbeat.
- Obtain and use local administrator rights to perform vCenter Server Heartbeat installation.
- Apply the latest Microsoft security updates.
- All applications that will be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.
- Verify that both Primary and Secondary servers have identical system date, time, and time Zone settings. Once configured, do not change the time zone.
- Verify that the Principal (Public) network adapter is listed as the first network adapter in the Network Connections Bind Order. (**Network Connections** > **Advanced > Advanced Settings**).
- Verify that the Managed IP setting in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Principal (Public) IP address.

Server Architecture Options

The selected server architecture affects the requirements for hardware and the technique used to clone the Primary server.

Virtual to Virtual (V2V)

V2V is the supported architecture if vCenter Server is already installed on the production (Primary) server running on a virtual machine. Benefits to this architecture include reduced hardware cost, shorter installation time, and use of the Pre-Clone technique for installation.

The Secondary virtual machine must meet the minimum requirements.

- The specifications of the Secondary virtual machine must match the specifications of the Primary virtual machine as follows:
  - Similar CPU (including resource management settings)
  - Memory configuration (including resource management settings)
  - Appropriate resource pool priorities
- Each virtual machine used in the V2V pair must be on a separate ESX host to guard against failure at the host level.
- Each virtual NIC must use a separate virtual switch.

Physical to Virtual (P2V)

P2V architecture is used when the environment requires a mix of physical and virtual machines, such as when vCenter Server is installed on a physical server in an environment where available hardware is limited. This architecture is appropriate if you must avoid adding more physical servers or if you plan to migrate to virtual technologies over a period of time. With P2V architecture, you can test vCenter Server running in a virtual environment or migrate from Physical to Virtual without any downtime. The Secondary virtual machine must meet the minimum requirements.

- The specifications of the Secondary virtual machine must match the Primary physical server as follows:
  - Similar CPU
  - Identical Memory
- The Secondary virtual machine must have sufficient priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Physical to Physical (P2P)

P2P architecture is used in environments where both the Primary and Secondary servers are physical servers. Use of P2P limits installation options as it requires use of the Install Clone technique. This architecture requires attention to detail when preparing for installation as both hardware and software must meet specific prerequisites.

Primary Server

The Primary server must meet the following requirements:

- Hardware as specified in "Common Requirements" on page 22.
- Software as specified in "Common Requirements" on page 22.

Secondary Server

The Secondary server operates as a near clone of the Primary server and must meet the following requirements.

Hardware

Hardware should be equivalent to the Primary server to ensure adequate performance when the server is in the active role:

- Similar CPU.
- Similar memory.
- Identical number of NICs to the Primary server.
- Drive letters must match the Primary server.
- Available disk space must be greater than or equal to the Primary server.
- Advanced Configuration and Power Interface (ACPI) compliance must match the Primary server. The vCenter Server Heartbeat Standard implementation process assumes identical ACPI compliance on both machines. If not, contact VMware Support at www.vmware.com/support for further information.

Software

Software on the Secondary server must meet the following requirements.

- OS version and Service Pack version must match the Primary server.
- OS must be installed to the same driver letter and directory as on the Primary server.
- Machine name must be different from the Primary server prior to installing vCenter Server Heartbeat.
- Set up in a workgroup prior to installing vCenter Server Heartbeat.
- System date, time, and time zone settings must be consistent with the Primary server.

Cloning Technology Options

Cloning the Primary server to create a nearly identical Secondary server involves different techniques depending on the selected server architecture.

Supported Pre-Clone Technologies

The following cloning technologies are supported for creating Pre-Cloned images for use as a Secondary server:

- VMware Converter for "Physical to Virtual (P2V)" on page 23.
- VMware vCenter virtual machine cloning for "Virtual to Virtual (V2V)" on page 22.

Supported Install Clone Technologies

Installation of vCenter Server Heartbeat provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated Install Cloning. This process is automated but requires meeting all prerequisites for the Secondary server specified in "Physical to Physical (P2P)" on page 23.

Application Component Options

vCenter Server Heartbeat can accommodate any of the supported vCenter Server configurations and protects the following components:

- VirtualCenter Server Version 2.5
  - VMware VirtualCenter Server
  - VMware Capacity Planner
  - VMware Converter Enterprise
  - VMware Update Manager
  - VMware License Server
- vCenter Server Version 4.0
  - VMware vCenter Server
  - VMware Guided Consolidation Service
  - VMware License Sever
  - VMware ADAM
  - VMware vCenter Management Web Server
  - VMware Update Manager
  - VMware Converter Enterprise
  - Guided Consolidation Service
  - VMware Orchestrator
  - VMware vSphere Host Update Utility

NOTE Ensure that all VMware components are bound to the Principal (Public) IP address on the Principal (Public) network adapter and that the Principal (Public) network adapter is listed first in the bind order of the **Network Connections** > **Advanced > Advanced Settings** window.

vCenter Server with SQL Server on the Same Host

To ensure adequate performance in 20+ host or 200+ virtual machine environments, VMware recommends that SQL Server and vCenter Server be installed on separate physical disk drives. VMDKs must be on separate datastores to avoid potential disk bottlenecks.

vCenter Server with SQL Server on a Separate Host

When installing vCenter Server Heartbeat in an environment where SQL Server is on a separate host from vCenter Server, repeat the installation process for the Primary and Secondary server specifically for the SQL Server.

To ensure proper failover, increase the default Heartbeat interval for the vCenter Server from 20 to 30 seconds.

vCenter Server Only

The **vCenter Server Only** option requires a single iteration of the installation process because the database is not protected.

Network Options

Networking requirements are contingent on how vCenter Server Heartbeat is deployed. To deploy as a High Availability (HA) solution, a LAN configuration is required. To deploy vCenter Server Heartbeat for Disaster Recovery (DR), a WAN configuration is required. Each network configuration has specific configuration requirements to ensure proper operation.

LAN

When deployed in a LAN environment, vCenter Server Heartbeat requires that both servers use the same Principal (Public) IP address. Each server also requires a separate VMware Channel IP address on a separate dedicated subnet.

NOTE When installing vCenter Server Heartbeat in a LAN environment, do not enable the Low Bandwidth Module as this is designed for WAN deployments.

Primary Server

Three NICs (1 x Public and 2 x Channel) are recommended for redundancy in the event one channel fails. A minimum of two NICs (one for the Channel, and one for the Public) are required in this configuration. Split-brain Avoidance should be configured.

- Principal (Public) network connection configured with the following:
  - Static IP address
  - Correct network mask
  - Correct Gateway address
  - Correct preferred and secondary (if applicable) DNS server address
  - NetBIOS enabled
- Channel Network connection(s) configured with the following:
  - Static IP address in a different subnet than the Principal (Public) network with a different IP address than the Secondary server channel NIC
  - Correct network mask
  - No Gateway IP address
  - No DNS server address
  - NetBIOS enabled (setup will disable this during the installation process)

Secondary Server

Networking components on the Secondary server must be configured as follows:

- Same number of NICs as the Primary server
- Principal (Public) network connection configured with temporary network settings
- Channel network connection(s) configured with the following:
  - Static IP address in a different subnet than the Principal (Public) network with a different IP address than the Primary server channel NIC
  - Correct network mask
  - No Gateway IP address
  - No DNS IP address
  - NetBIOS enabled (setup will disable this during the installation process
  - File and print sharing enabled

WAN

Deploying vCenter Server Heartbeat in a WAN environment requires additional considerations. Each server within the vCenter Server Heartbeat pair requires its own separate Principal (Public) IP address and a VMware Channel IP address in a separate dedicated subnet.

WAN Requirements

WAN deployments require the following:

- Persistent static routing configured for the channel connection(s) where routing is required
- Two NICs (1 x Public and 1 x Channel) are recommended
- At least one Domain Controller at the Disaster Recovery (DR) site
- If the Primary and DR site use the same subnet:
  - During install, follow the steps for a LAN or VLAN on the same subnet
  - Both servers in the vCenter Server Heartbeat pair use the same Public IP address
- If the Primary and DR site use different subnets:
  - During install, follow the steps for a WAN
  - Both servers in the vCenter Server Heartbeat pair require a separate Principal (Public) IP address and a VMware Channel IP address in a separate dedicated subnet
  - Provide a user account with rights to update DNS using the DNSUpdate utility provided as a component of vCenter Server Heartbeat through vCenter Server Heartbeat Console **Application** > **Task** > **User Accounts**
  - VMware recommends integrating Microsoft DNS into AD so that DNSUpdate can identify all DNS Servers that require updating
  - At least one Domain Controller at the DR site
  - Refer to the following articles in the VMware Knowledge Base:
    - KB 1008571 – *Configuring DNS in a WAN Environment*
    - KB 1008605 – *Configuring vCenter Server Heartbeat to Update BIND9 DNS Servers Deployed in a WAN*

Bandwidth

Determine the available bandwidth and estimate the required volume of data throughput to determine acceptable latency for the throughput. Additionally, the bandwidth can affect the required queue size to accommodate the estimated volume of data. VMware recommends making a minimum of 1Mbit of spare bandwidth available to vCenter Server Heartbeat.

vCenter Server Heartbeat includes a Low Bandwidth Module for use in WAN environments. When enabled, the VMware Channel compresses the data, optimizing the traffic for low bandwidth connections causing some additional CPU load on the active server.

Latency

Latency has a direct effect on data throughput. Latency on the link should not fall below the standard defined for a T1 connection.

Heartbeat Diagnostics can assist in determining the available bandwidth, required bandwidth, and server workload. For more information about Heartbeat Diagnostics, contact VMware Professional Services.

Antivirus Recommendations

Consult with and implement the advice of your antivirus (AV) provider, as VMware guidelines often follow these recommendations. Consult the VMware knowledge base for up to date information on specific AV products.

Do not use file level AV to protect application server databases, such as MS SQL Server databases. The nature of database contents can cause false positives in virus detection, leading to failed database applications, data integrity errors, and performance degradation.

VMware recommends that when implementing vCenter Server Heartbeat, you do not replicate file level AV temp files using vCenter Server Heartbeat.

The file level AV software running on the Primary server must be the same as the software that runs on the Secondary server. In addition, the same file level AV must run during both active and passive roles.

Configure file level AV to use the management IP address on the passive server for virus definition updates. If this is not possible, manually update virus definitions on the passive server.

Exclude the following VMware directories from file level AV scans (`C:\Program Files\VMware\VMware vCenter Server Heartbeat\` is the default installation directory):

- `C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\logs`
- `C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\log`

Any configuration changes made to a file level AV product on one server (such as exclusions) must be made on the other server as well. vCenter Server Heartbeat does not replicate this information.

Deployment Options Summary

Table 2-1 provides all possible deployment options described in this section.

Table 2-1. Installation Options

	Network		Clone Technique		Component		
	LAN	**WAN**	**Pre-Clone**	**InstallClone**	**vCenter Server w/SQL Local**	**vCenter Server w/SQL Remote**	**vCenter Server Only**
V2V	X	X	X	-	X	X	X
P2V	X	X	X	X	X	X	X
P2P	X	X	-	X	X	X	X

Installation Options Checklist

Verify the prerequisites:

Server architecture:

___ P2P

___ P2V

___ V2V

Cloning technology option:

___ Pre-Clone Install

___ Install Clone

Application components to protect:

___ vCenter Server with SQL Server on same host

___ vCenter Server with SQL Server on separate host

___ vCenter Server only

Network environment type:

___ LAN

___ WAN

Is the subnet the same at the Secondary site?

- If Yes, an IP address is required for this subnet

Active Directory Integrated DNS?

- If Yes, a Domain Account with rights to update DNS is required.
- If No, refer to the knowledge base articles in "Network Options" on page 25.

vCenter Server Heartbeat Installation on Windows Server 2003

3

This chapter includes the following topics:

- "Overview" on page 31
- "Installation Process" on page 31
- "Primary Server" on page 32
- "Secondary Server" on page 53
- "Post Installation Configuration" on page 68

Overview

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2003. During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. Should the server fail one of the checks, a critical stop or warning message appears. Refer to the Appendix – Setup Error Messages in this guide for a list of the checks and an explanation of the message. You must resolve critical stops before you can proceed with setup.

Prior to installing vCenter Server Heartbeat, you must identify the deployment options you want. The installation process requires you to select options throughout the procedure to achieve your configuration goals.

Installation Process

After selecting implementation options, begin the installation process. The installation process for all scenarios follows the same basic procedure. Links to specific installation scenarios describing differences are identified by the blue hyperlinked text.

Primary Server

Installation of vCenter Server Heartbeat begins on the Primary server.

NOTE vCenter Server Heartbeat installs in the evaluation mode. Refer to "Post Installation Configuration" on page 68 for instructions on how to enter a production serial number.

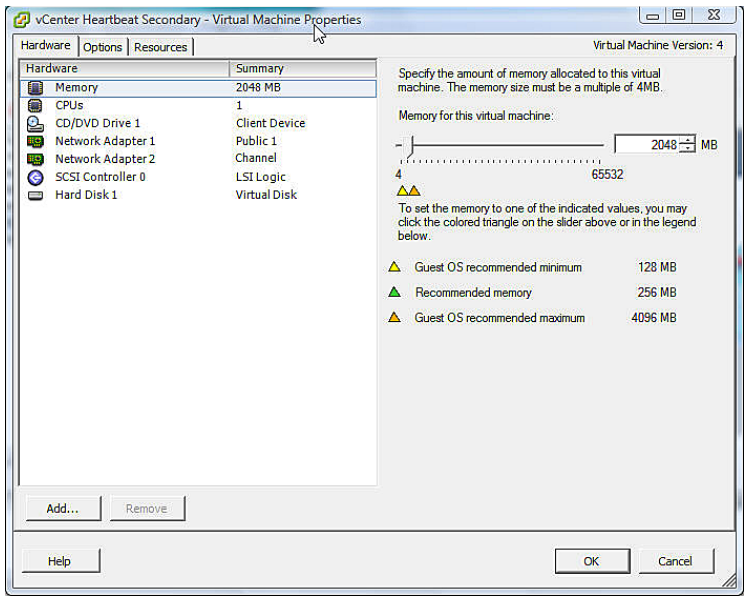
1 Having verified all of the environmental prerequisites are met, download vCenter Server Heartbeat the WinZip self extracting file to an appropriate location on the Primary server (either Physical or Virtual).

You have the following options:

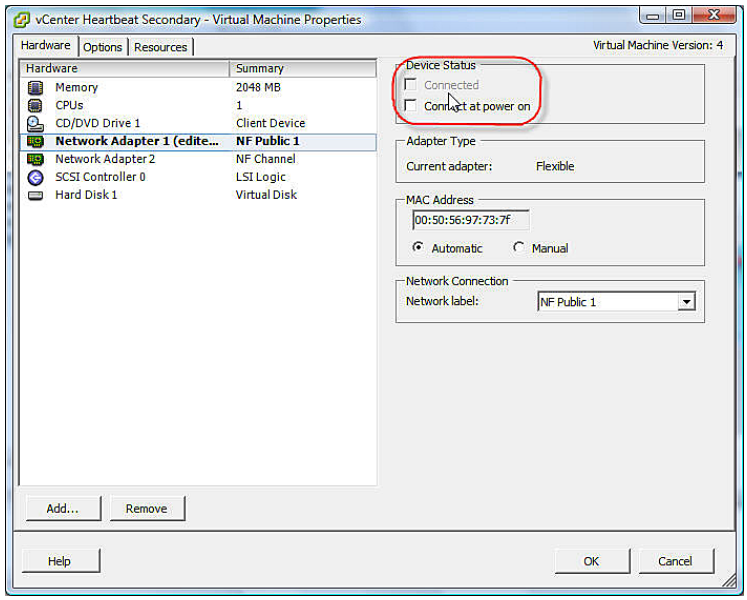
- For P2P, go to Step 2 to continue the installation.
- For V2V or P2V installations with the Pre-Clone technique selected, begin with Step a below to configure the network settings on the Secondary server.

a Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third-party utility to create a cloned image of the Primary server. The clone must be completely identical with no changes to the Name, SID, or domain membership.

b After creating the cloned image, but before powering on the cloned image, edit the image settings.



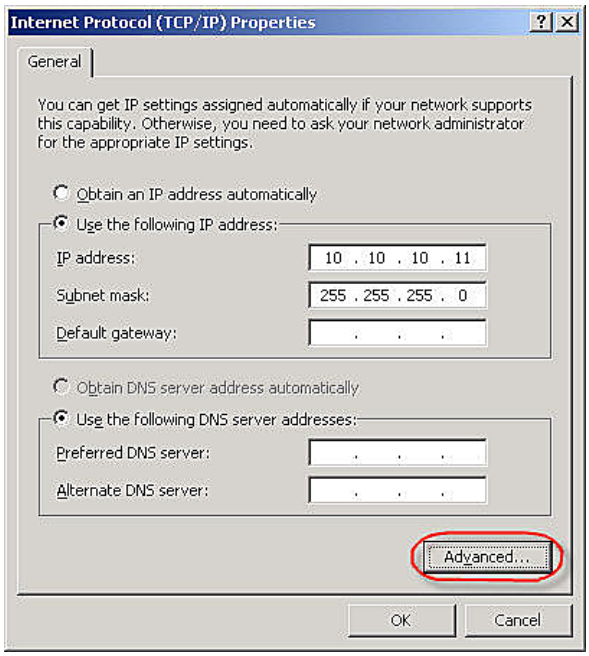
c Select the Public virtual network adapter and clear the **Connected** and **Connect at power on** check boxes.



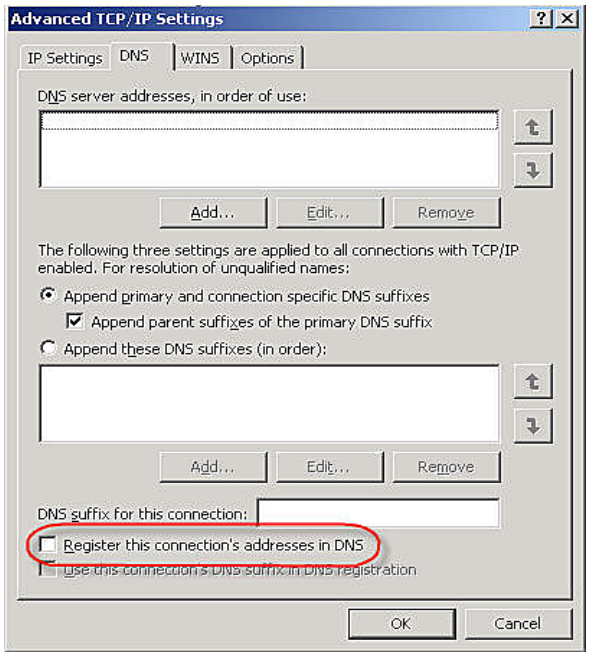
d Repeat the process on the Channel virtual network adapter.

e Power on the Secondary (previously cloned) server image.

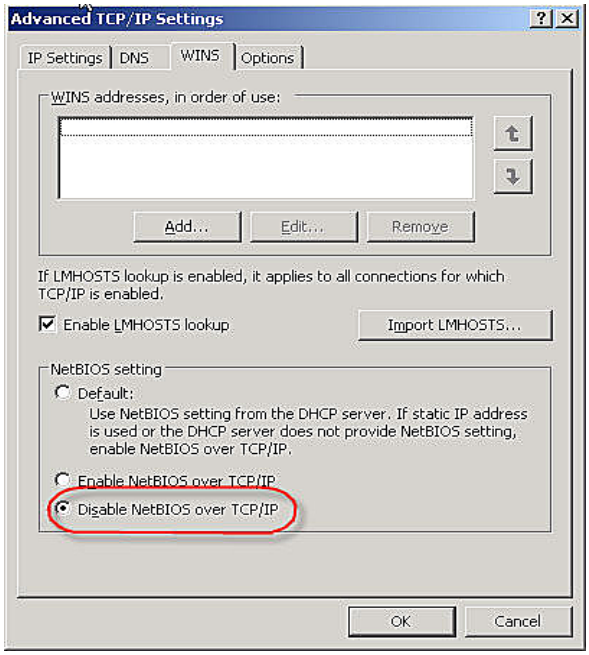
f After the Secondary starts, open Network Connections, right-click the VMware Channel network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 10 . 10 . 11
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

g Configure the appropriate VMware Channel IP address and subnet mask. Click **Advanced...**



h Click the **DNS** tab, clear the **Register this connection's addresses in DNS** check box, and click **OK**.


Advanced TCP/IP Settings
IP Settings
DNS
WINS
Options
WINS addresses, in order of use:
Add...
Edit...
Remove
If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.
Enable LMHOSTS lookup
Import LMHOSTS...
NetBIOS setting
Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
Enable NetBIOS over TCP/IP
Disable NetBIOS over TCP/IP
OK
Cancel

i Click the WINS tab, select **Disable NetBIOS over TCP/IP** and click **OK** twice.

j Select the Principal (Public) network connection, right-click and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Set the appropriate IP address (same as the Primary server for LAN installations), Subnet Mask, and Default Gateway, and click **OK**.

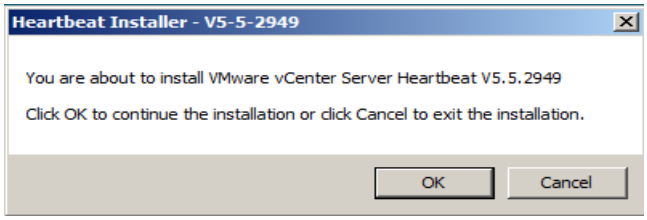
k In Network Connections, click **Advanced** and select **Advanced Settings**. Verify that the Principal (Public) NIC IP address is listed first in the Bind Order, and click **OK**.

l Right-click the Secondary (cloned) server image and select **Edit Settings**.

m Select the VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. IP communications with the Secondary server go through the VMware Channel.

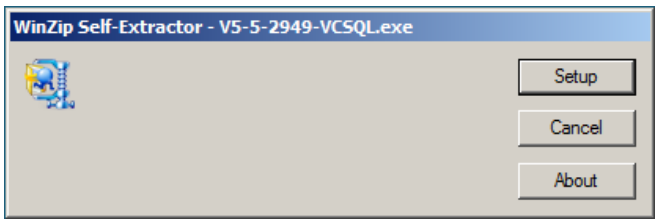
NOTE Do not connect the Principal (Public) virtual network adapter at this time to prevent an IP address conflict on the network.

2 Double click the WinZip Self Extracting file to initiate the installation process. The **Setup Introduction** window appears. Review the information and click **OK**.

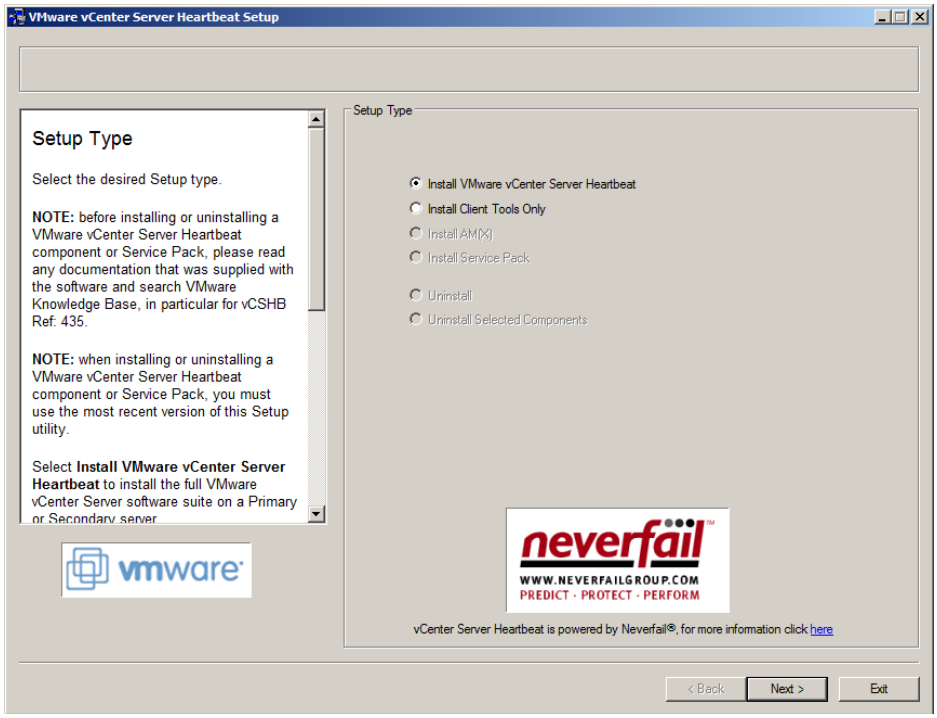

Heartbeat Installer - V5-5-2949
You are about to install VMware vCenter Server Heartbeat V5.5.2949
Click OK to continue the installation or click Cancel to exit the installation.
OK
Cancel

NOTE If you click **Exit** after Setup has started, you are prompted to save your settings. When you run `Setup.exe` later, you will be asked if you want to use the previously saved configuration.

3 The **WinZip Self-Extractor** window appears. Click **Setup** to continue.

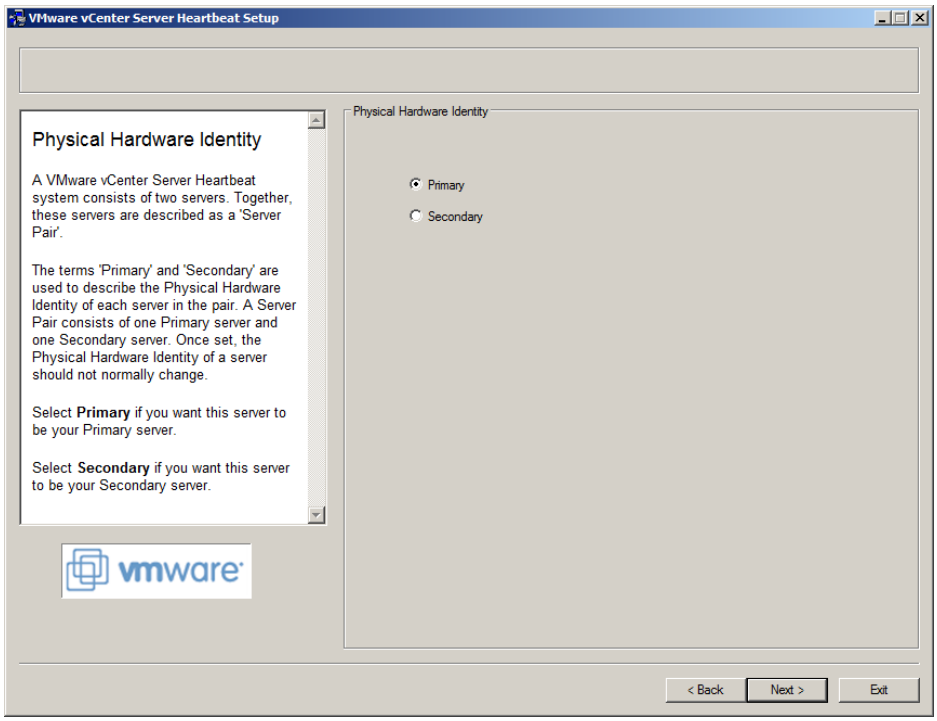


4 The **Setup Type** window appears. Because this is a new installation of vCenter Server Heartbeat, select **Install vCenter Server Heartbeat** and click Next.


VMware vCenter Server Heartbeat Setup
Setup Type
Select the desired Setup type.
NOTE: before installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, please read any documentation that was supplied with the software and search VMware Knowledge Base, in particular for vCSHB Ref: 435.
NOTE: when installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, you must use the most recent version of this Setup utility.
Select Install VMware vCenter Server Heartbeat to install the full VMware vCenter Server software suite on a Primary or Secondary server
Setup Type
Install VMware vCenter Server Heartbeat
Install Client Tools Only
Install AM(X)
Install Service Pack
Uninstall
Uninstall Selected Components
vmware
neverfail
WWW.NEVERFAILGROUP.COM
PREDICT · PROTECT · PERFORM
vCenter Server Heartbeat is powered by Neverfail®, for more information click here
< Back
Next >
Exit

NOTE The left pane of each page in the setup wizard provides information about the setup process.

5 Select the identity of the server on the **Physical Hardware Identity** page. Select **Primary** as the server identity and click **Next**.


VMware vCenter Server Heartbeat Setup
Physical Hardware Identity
A VMware vCenter Server Heartbeat system consists of two servers. Together, these servers are described as a 'Server Pair'.
The terms 'Primary' and 'Secondary' are used to describe the Physical Hardware Identity of each server in the pair. A Server Pair consists of one Primary server and one Secondary server. Once set, the Physical Hardware Identity of a server should not normally change.
Select Primary if you want this server to be your Primary server.
Select Secondary if you want this server to be your Secondary server.
vmware
Physical Hardware Identity
Primary
Secondary
< Back
Next >
Exit

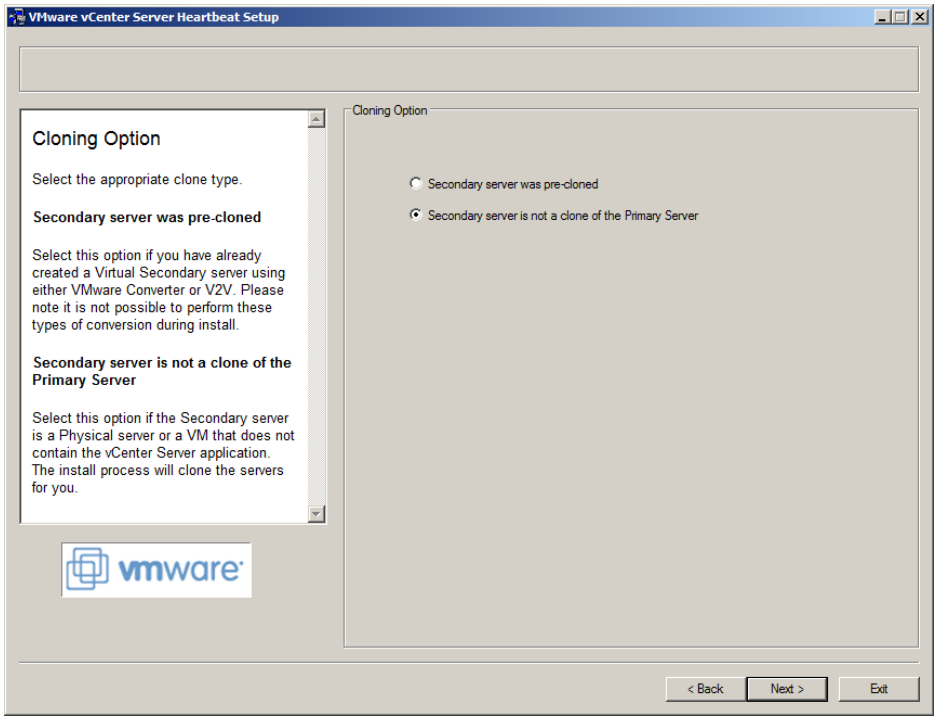
NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

Select the cloning options. If using the Install Clone technique, go to Step 6. If using the Pre-Clone technique, click the link below to jump to the Pre-Clone technique instructions.

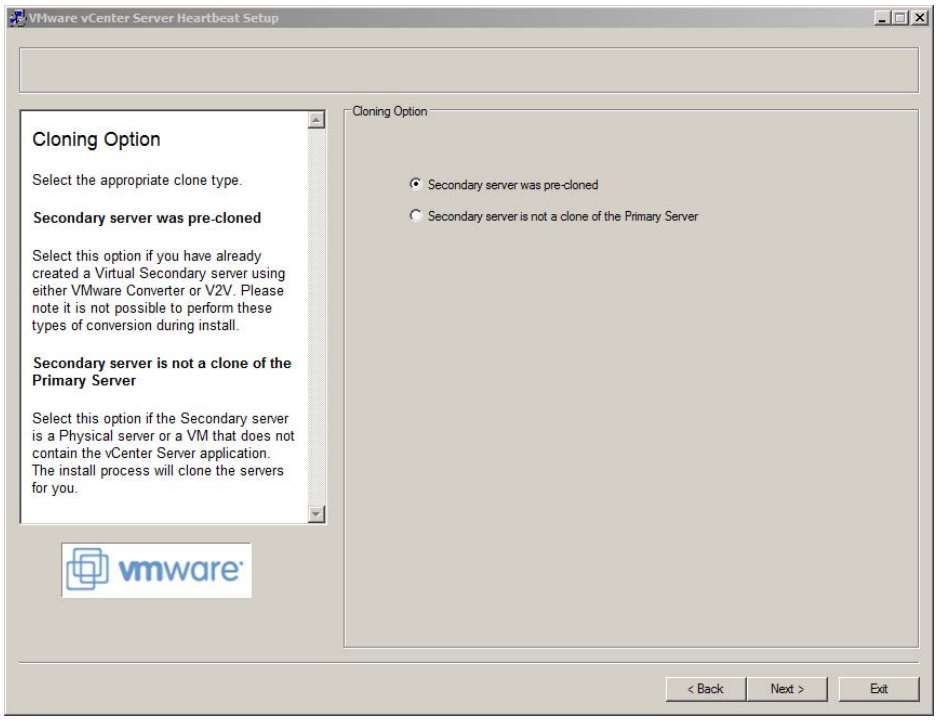
You have the following options:

- For installation using the Install Clone technique, continue with Step 6.
- For installation using the Pre-Clone technique, continue with Step 7.

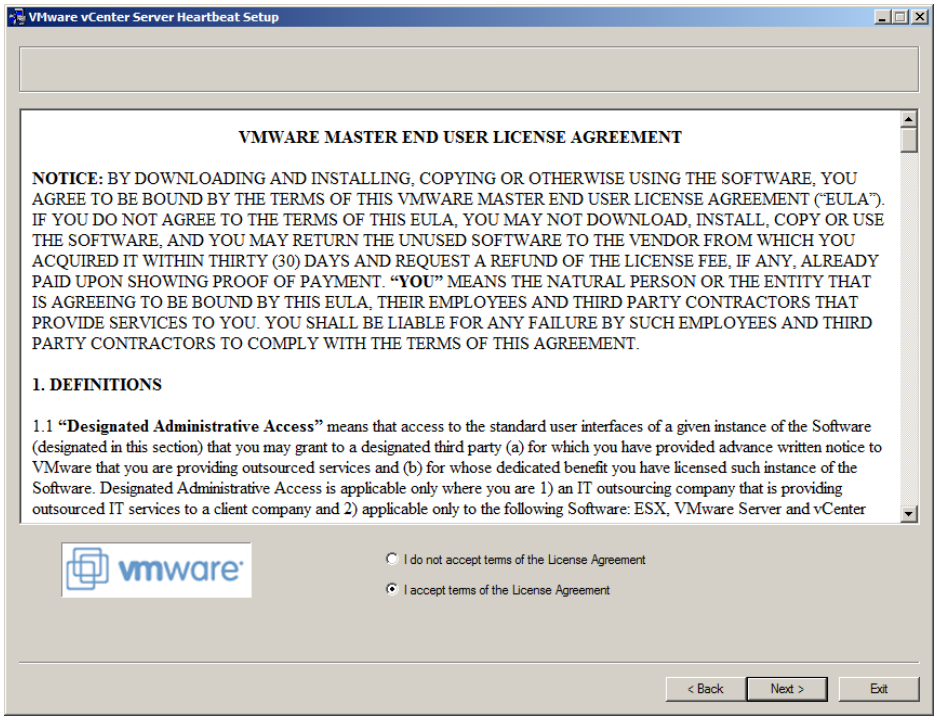
6 Select **Secondary server is not a clone of the Primary server**, click **Next,** and go to Step 8.


VMware vCenter Server Heartbeat Setup
Cloning Option
Select the appropriate clone type.
Secondary server was pre-cloned
Select this option if you have already created a Virtual Secondary server using either VMware Converter or V2V. Please note it is not possible to perform these types of conversion during install.
Secondary server is not a clone of the Primary Server
Select this option if the Secondary server is a Physical server or a VM that does not contain the vCenter Server application. The install process will clone the servers for you.
Cloning Option
Secondary server was pre-cloned
Secondary server is not a clone of the Primary Server
vmware
< Back
Next >
Exit

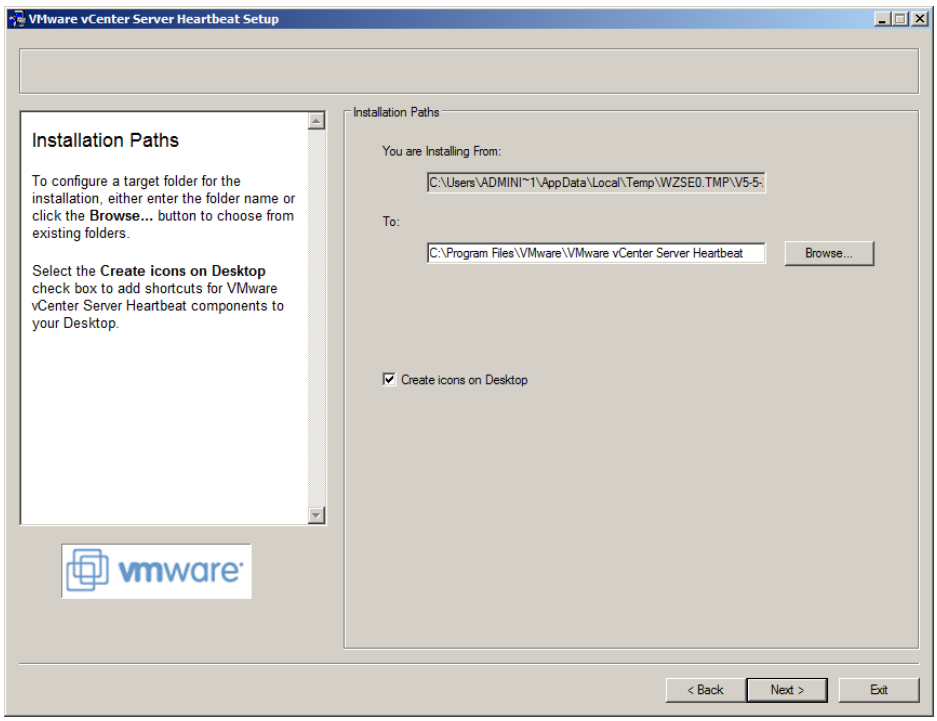
7 If a virtual Secondary server was created using VMware Converter, the cloning option in the Virtual Infrastructure Client, or a third-party utility, select **Secondary server was pre-cloned** and click **Next**.


VMware vCenter Server Heartbeat Setup
Cloning Option
Select the appropriate clone type.
Secondary server was pre-cloned
Select this option if you have already created a Virtual Secondary server using either VMware Converter or V2V. Please note it is not possible to perform these types of conversion during install.
Secondary server is not a clone of the Primary Server
Select this option if the Secondary server is a Physical server or a VM that does not contain the vCenter Server application. The install process will clone the servers for you.
Cloning Option
Secondary server was pre-cloned
Secondary server is not a clone of the Primary Server
vmware
< Back
Next >
Exit

8 Read the license agreement carefully and select **I accept the terms of the License Agreement**. Click **Next**.


VMware vCenter Server Heartbeat Setup
VMWARE MASTER END USER LICENSE AGREEMENT
NOTICE: BY DOWNLOADING AND INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS VMWARE MASTER END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT DOWNLOAD, INSTALL, COPY OR USE THE SOFTWARE, AND YOU MAY RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, ALREADY PAID UPON SHOWING PROOF OF PAYMENT. "YOU" MEANS THE NATURAL PERSON OR THE ENTITY THAT IS AGREEING TO BE BOUND BY THIS EULA, THEIR EMPLOYEES AND THIRD PARTY CONTRACTORS THAT PROVIDE SERVICES TO YOU. YOU SHALL BE LIABLE FOR ANY FAILURE BY SUCH EMPLOYEES AND THIRD PARTY CONTRACTORS TO COMPLY WITH THE TERMS OF THIS AGREEMENT.
1. DEFINITIONS
1.1 "Designated Administrative Access" means that access to the standard user interfaces of a given instance of the Software (designated in this section) that you may grant to a designated third party (a) for which you have provided advance written notice to VMware that you are providing outsourced services and (b) for whose dedicated benefit you have licensed such instance of the Software. Designated Administrative Access is applicable only where you are 1) an IT outsourcing company that is providing outsourced IT services to a client company and 2) applicable only to the following Software: ESX, VMware Server and vCenter
vmware
I do not accept terms of the License Agreement
I accept terms of the License Agreement
< Back
Next >
Exit

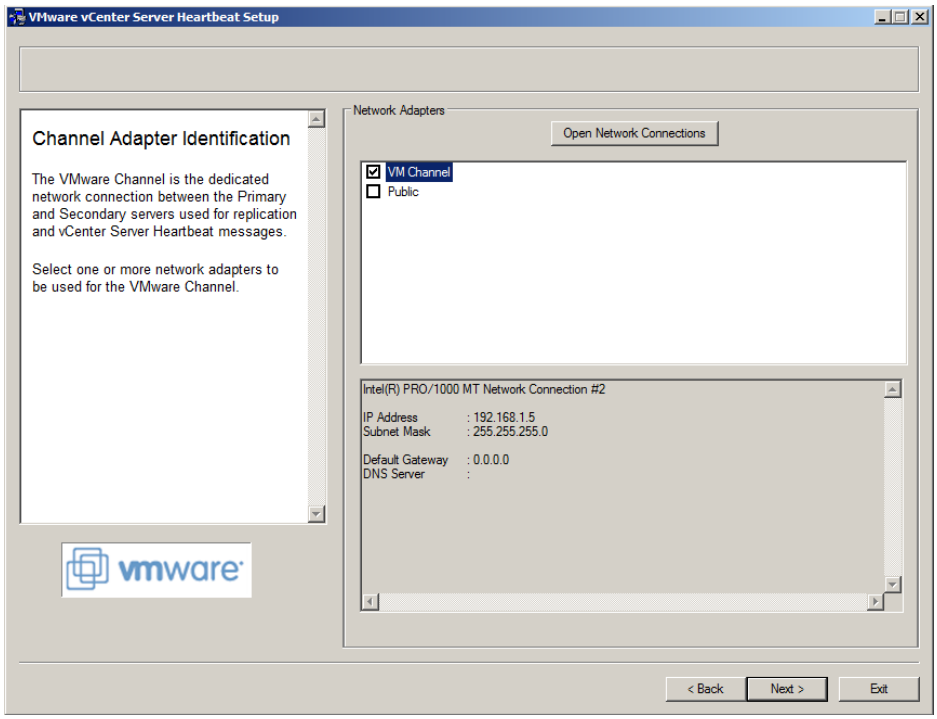
9 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.


VMware vCenter Server Heartbeat Setup
Installation Paths
To configure a target folder for the installation, either enter the folder name or click the Browse... button to choose from existing folders.
Select the Create icons on Desktop check box to add shortcuts for VMware vCenter Server Heartbeat components to your Desktop.
Installation Paths
You are Installing From:
C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-
To:
C:\Program Files\VMware\VMware vCenter Server Heartbeat
Browse...
Create icons on Desktop
vmware
< Back
Next >
Exit

NOTE The path of the VMware installation folder cannot contain Unicode characters. If vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, this causes the Neverfail Server R2 service to fail to start. The path of the VMware installation folder can only contain lower and upper case letters A to Z, digits from 0 to 9, and the following special characters: space \ _ - ( ) . :

Alternatively, click **Browse** to select one of these locations. Select **Create icons on Desktop** and click **Next**.

10 Identify the network adapter(s) for use in the VMware Channel on the **Channel Adapter Identification** page. Select the network adapters (NICs) for the VMware Channel from the list. Click the adapter name to display the selected NIC properties in the lower panel. You must select at least one NIC to proceed with the installation.

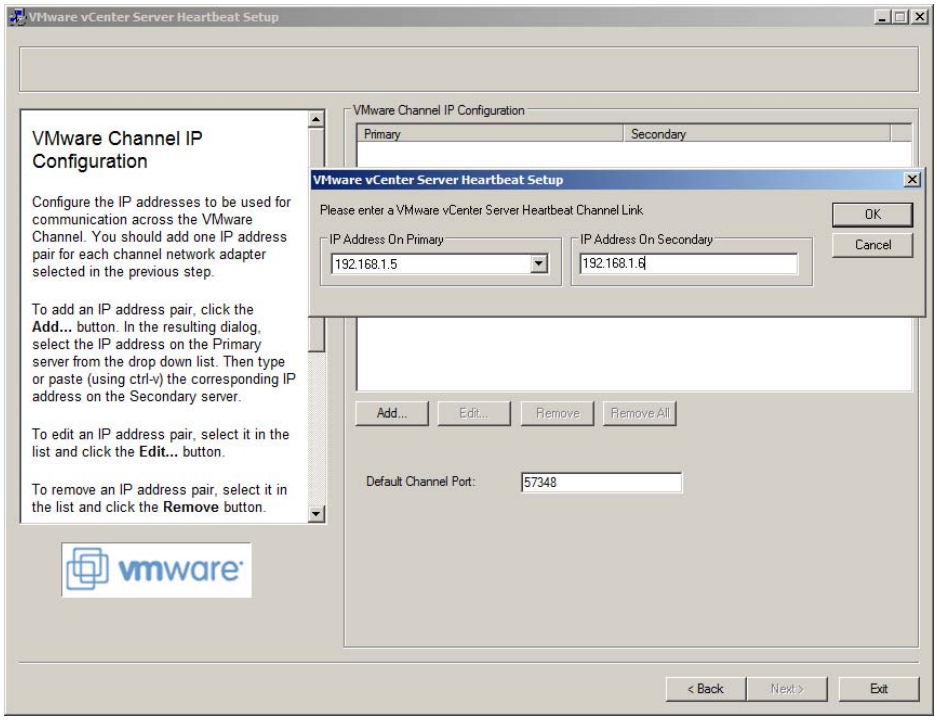

VMware vCenter Server Heartbeat Setup
Channel Adapter Identification
The VMware Channel is the dedicated network connection between the Primary and Secondary servers used for replication and vCenter Server Heartbeat messages.
Select one or more network adapters to be used for the VMware Channel.
vmware
Network Adapters
Open Network Connections
VM Channel
Public
Intel(R) PRO/1000 MT Network Connection #2
IP Address : 192.168.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
DNS Server :
< Back
Next >
Exit

11 If no NICs are available, click **Open Network Connections** to review the network configuration of your machine and verify that you have the correct number of NICs installed.

NOTE Only one channel can be configured for each NIC. To configure more than one channel you must identify more than one NIC. A disabled NIC does not appear in this list. Enable the NIC to display it. If a NIC is disconnected, its IP addresses do not appear in the lower panel.

---

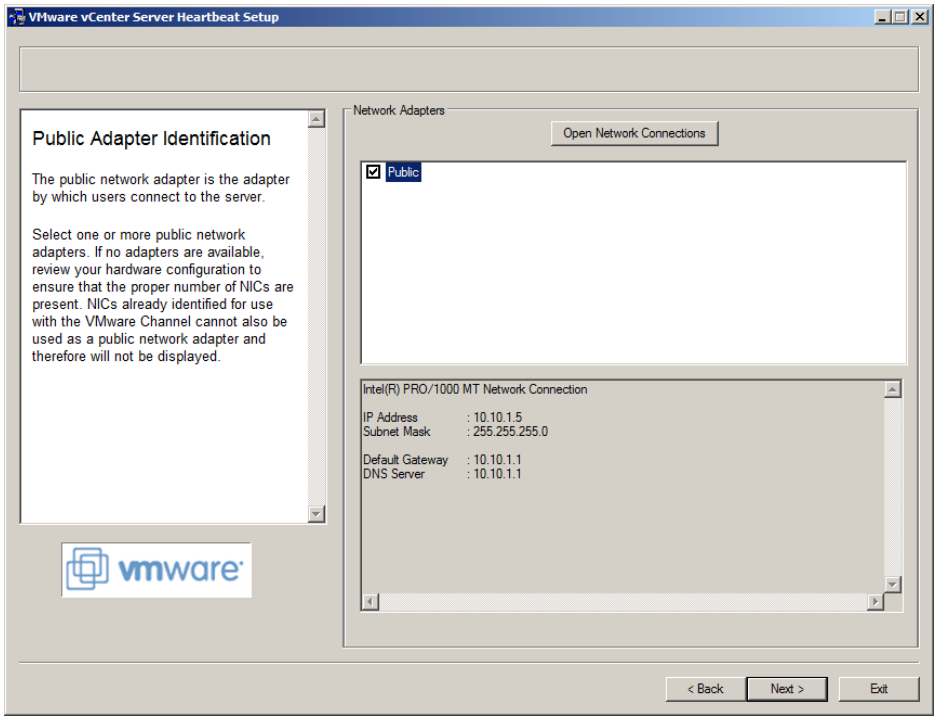
12 The **VMware Channel IP Configuration** page prompts you to configure the VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. For the Primary server, select from a drop-down menu that lists all local IP addresses. Type the reciprocal IP address on the Secondary server into the **IP Address On Secondary** text box. You must specify all VMware Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card. Click **OK**. Repeat this step for additional NICs.


VMware vCenter Server Heartbeat Setup
VMware Channel IP Configuration
Configure the IP addresses to be used for communication across the VMware Channel. You should add one IP address pair for each channel network adapter selected in the previous step.
To add an IP address pair, click the Add... button. In the resulting dialog, select the IP address on the Primary server from the drop down list. Then type or paste (using ctrl-v) the corresponding IP address on the Secondary server.
To edit an IP address pair, select it in the list and click the Edit... button.
To remove an IP address pair, select it in the list and click the Remove button.
vmware
VMware Channel IP Configuration
Primary
Secondary
VMware vCenter Server Heartbeat Setup
Please enter a VMware vCenter Server Heartbeat Channel Link.
OK
Cancel
IP Address On Primary
192.168.1.5
IP Address On Secondary
192.168.1.6
Add...
Edit...
Remove
Remove All
Default Channel Port:
57348
< Back
Next >
Exit

13 Review and adjust, if necessary, the default channel port. Click **Next**.

NOTE When the implementation spans multiple sites with firewalls between the servers, configure the firewalls to allow traffic to pass through the default channel port or the manually configured channel port. Consult the VMware knowledge base for additional information.

14 Select the Principal (Public) NIC(s). The IP address information is displayed for each NIC.


VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
vmware
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
< Back
Next >
Exit

vCenter Server Heartbeat software can be deployed in a configuration where both servers have the same Principal (Public) IP address, for instance, in a standard Local Area Network (LAN) deployment where both machines are in the same subnet.

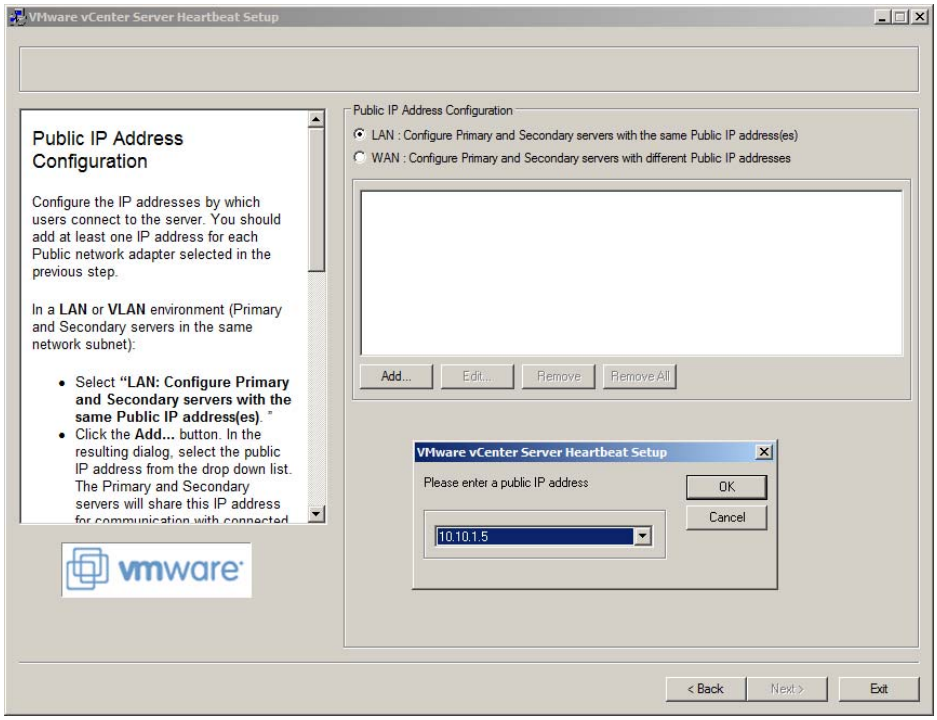
Alternatively vCenter Server Heartbeat can be deployed where the Principal (Public) IP addresses differ, for instance, in a Wide Area Network (WAN) deployment where the Primary and Secondary servers are located in different sites and subnets where client access is therefore bound by the standard network routing to allow the correct connectivity to the server according to its locale.

15 Select **LAN: Configure Primary and Secondary servers with the same Public IP addresses** or **WAN: Configure Primary and Secondary servers with different Public IP addresses**.

You have the following options:

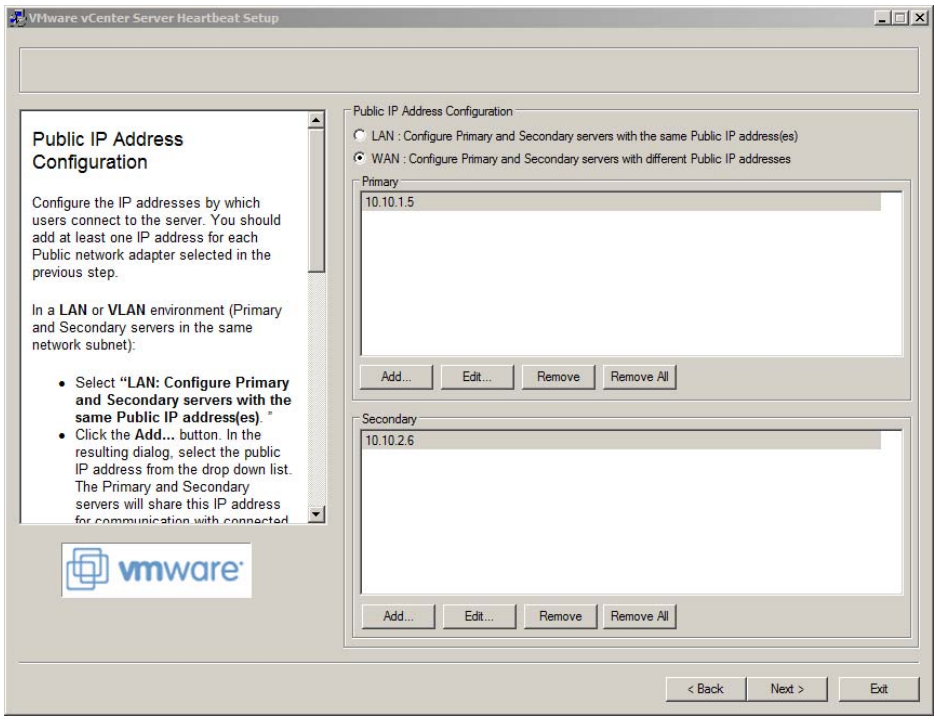
- For a WAN installation with different subnets, go to Step 17.
- For LAN installation or same subnet WAN installs, continue with Step 16.

16 For a LAN environment, click **Add** to specify the IP address.


VMware vCenter Server Heartbeat Setup
Public IP Address Configuration
Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Public network adapter selected in the previous step.
In a LAN or VLAN environment (Primary and Secondary servers in the same network subnet):
Select "LAN: Configure Primary and Secondary servers with the same Public IP address(es)."
Click the Add... button. In the resulting dialog, select the public IP address from the drop down list. The Primary and Secondary servers will share this IP address
Public IP Address Configuration
LAN : Configure Primary and Secondary servers with the same Public IP address(es)
WAN : Configure Primary and Secondary servers with different Public IP addresses
Add...
Edit...
Remove
Remove All
VMware vCenter Server Heartbeat Setup
Please enter a public IP address
OK
Cancel
10.10.1.5
vmware
< Back
Next >
Exit

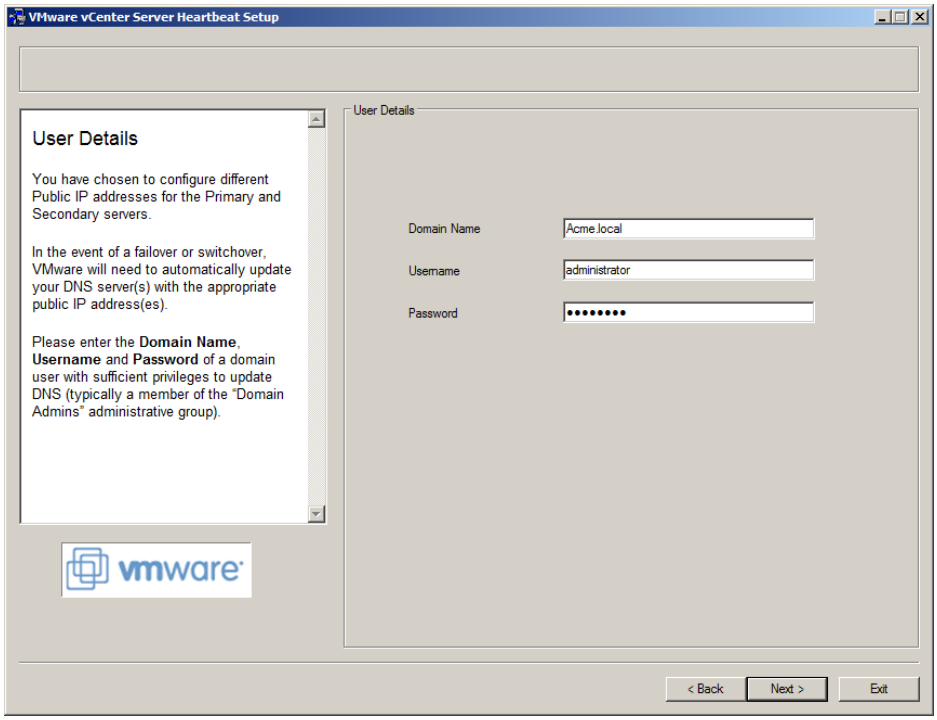
If installing in a LAN or when the WAN uses the same subnet, go to Step 20.

17 For a WAN environment, specify IP addresses of the Secondary server and the Primary server.


VMware vCenter Server Heartbeat Setup
Public IP Address Configuration
Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Public network adapter selected in the previous step.
In a LAN or VLAN environment (Primary and Secondary servers in the same network subnet):
Select "LAN: Configure Primary and Secondary servers with the same Public IP address(es)."
Click the Add... button. In the resulting dialog, select the public IP address from the drop down list. The Primary and Secondary servers will share this IP address
Public IP Address Configuration
LAN : Configure Primary and Secondary servers with the same Public IP address(es)
WAN : Configure Primary and Secondary servers with different Public IP addresses
Primary
10.10.1.5
Add...
Edit...
Remove
Remove All
Secondary
10.10.2.6
Add...
Edit...
Remove
Remove All
vmware
< Back
Next >
Exit

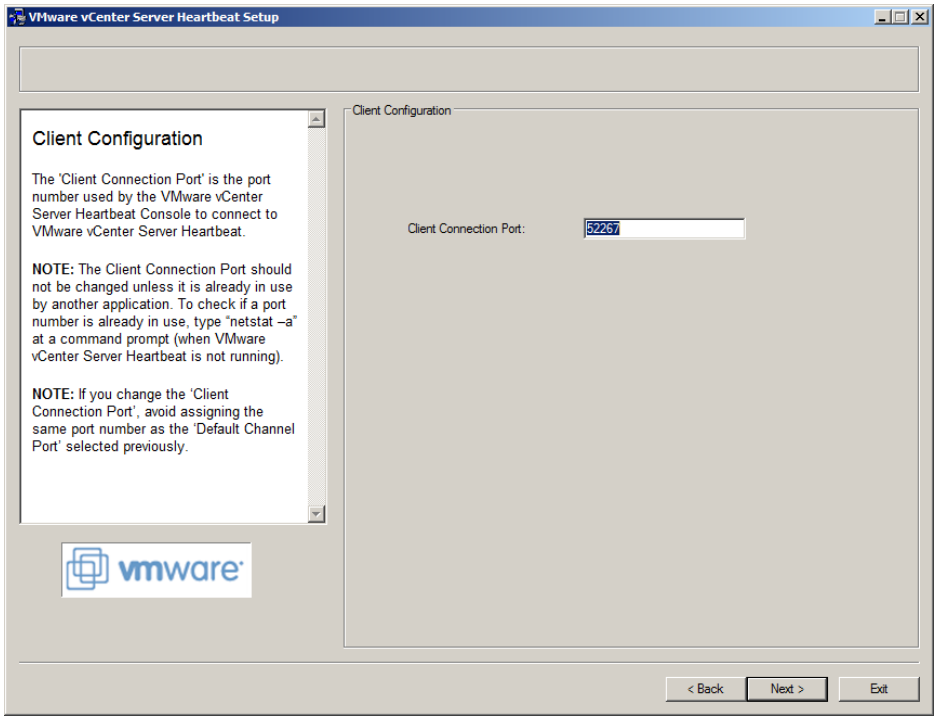
18 Add each Principal (Public) network address until all addresses are present. Click **Next**.

19 When the Principal (Public) addresses on the Secondary server are different from those on the Primary server, vCenter Server Heartbeat must perform additional tasks during failover or switchover. These additional tasks require clients to change their resolution of the active server to a different IP address and requires that vCenter Server Heartbeat update the DNS entries for the active server across the enterprise. Such updates require credentials for domain administrators (or an account with equivalent rights). Type the **Domain Name**, a domain administrator **Username** and **Password** in the respective text boxes and click **Next**.


VMware vCenter Server Heartbeat Setup
User Details
You have chosen to configure different Public IP addresses for the Primary and Secondary servers.
In the event of a failover or switchover, VMware will need to automatically update your DNS server(s) with the appropriate public IP address(es).
Please enter the Domain Name, Username and Password of a domain user with sufficient privileges to update DNS (typically a member of the "Domain Admins" administrative group).
vmware
User Details
Domain Name
Acme.local
Username
administrator
Password
< Back
Next >
Exit

The vCenter Server Heartbeat server pair can be administered remotely on client machines using the vCenter Server Heartbeat Console.

20 The vCenter Server Heartbeat Console connects to an IP address of the active server using the default client connection port of 52267. If this port is already in use, type an available client connection port in the text box. Click **Next**.


VMware vCenter Server Heartbeat Setup
Client Configuration
The 'Client Connection Port' is the port number used by the VMware vCenter Server Heartbeat Console to connect to VMware vCenter Server Heartbeat.
NOTE: The Client Connection Port should not be changed unless it is already in use by another application. To check if a port number is already in use, type "netstat –a" at a command prompt (when VMware vCenter Server Heartbeat is not running).
NOTE: If you change the 'Client Connection Port', avoid assigning the same port number as the 'Default Channel Port' selected previously.
vmware
Client Configuration
Client Connection Port:
52267
< Back
Next >
Exit

21 Select the applications to protect. All licensed vCenter Server Heartbeat features are listed.

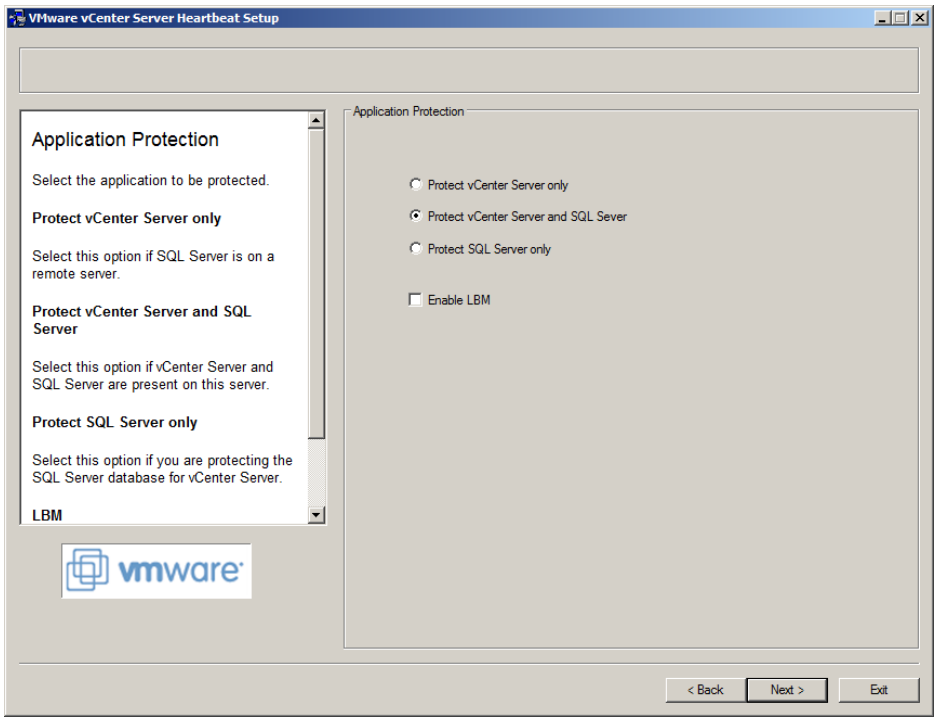
If installing vCenter Server only, or vCenter Server locally and the SQL Server on a separate server, select **Protect Virtual Center only**.

If installing SQL Server remotely, upon completion of the vCenter Server installation locally, repeat the installation procedure at the remote SQL Server location and select **Protect SQL Server only**.

If installing both vCenter Server and SQL Server locally, select **Protect Virtual Center and SQL Server**.

Select the applications to protect. If installing in a WAN, enable the Low Bandwidth Module by selecting **Enable LBM**. Click **Next**.

CAUTION Do not enable the Low Bandwidth Module (LBM) for a LAN install.


VMware vCenter Server Heartbeat Setup
Application Protection
Select the application to be protected.
Protect vCenter Server only
Select this option if SQL Server is on a remote server.
Protect vCenter Server and SQL Server
Select this option if vCenter Server and SQL Server are present on this server.
Protect SQL Server only
Select this option if you are protecting the SQL Server database for vCenter Server.
LBM
vmware
Application Protection
Protect vCenter Server only
Protect vCenter Server and SQL Sever
Protect SQL Server only
Enable LBM
< Back
Next >
Exit

22 Configure Microsoft Windows Backup options. To facilitate the clone of the Primary server onto the Secondary server, you must back up pertinent components of the Primary server for restoration on to the Secondary server.

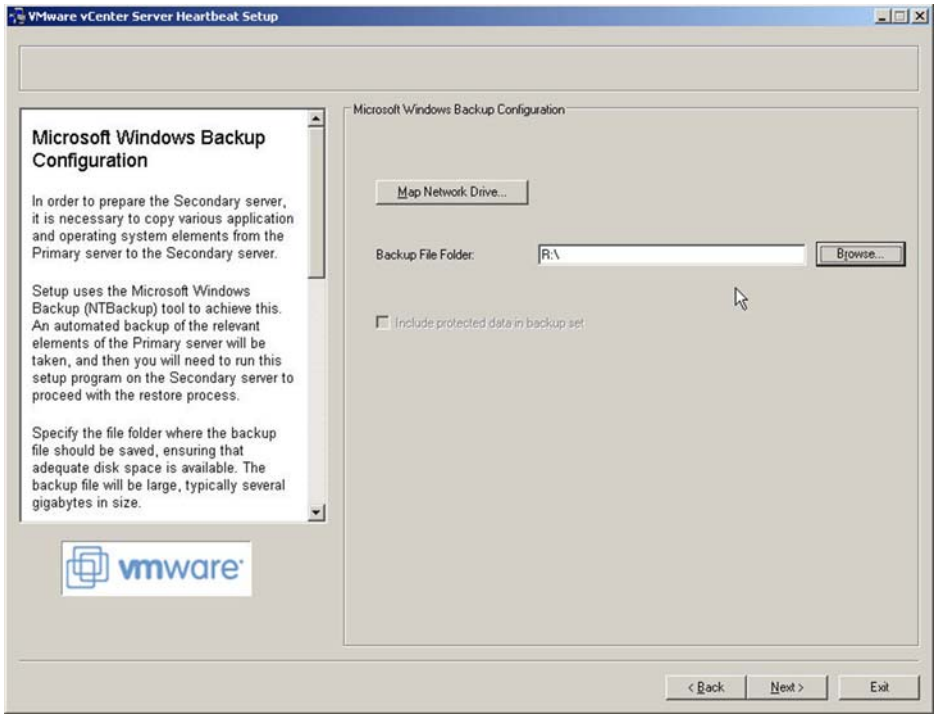
You have the following options:

- For installation using the Pre-Clone technique, go to Step 23 on page page 47.
- For installation using the Install Clone technique, continue with Step a.

Continue with Step a.

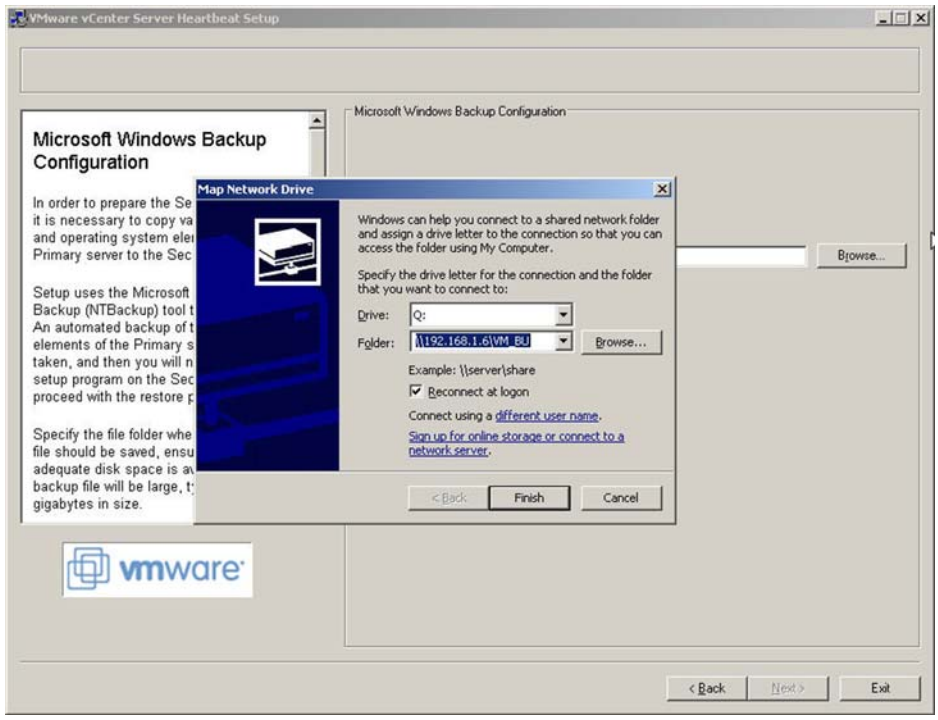
a Configure Microsoft Windows Backup options. Depending on the network topology between the servers, backup files can include or exclude application data. Including application data in the backup file decreases the time to initially verify and synchronize the applications data on first start up of vCenter Server Heartbeat. This is useful where VMware Channel connections are slower than LAN speed, such as in a WAN implementation.

With Windows Server 2003, vCenter Server Heartbeat does not stop services and prevents downtime by using the Windows Volume Shadow Service to take the backup. Including the applications' protected data greatly increases the backup file size and therefore increases the time of the backup operation. Due to the potential large size of the backup file, careful consideration is required when including application data and specifying the backup folder location.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Configuration
In order to prepare the Secondary server, it is necessary to copy various application and operating system elements from the Primary server to the Secondary server.
Setup uses the Microsoft Windows Backup (NTBackup) tool to achieve this. An automated backup of the relevant elements of the Primary server will be taken, and then you will need to run this setup program on the Secondary server to proceed with the restore process.
Specify the file folder where the backup file should be saved, ensuring that adequate disk space is available. The backup file will be large, typically several gigabytes in size.
vmware
Microsoft Windows Backup Configuration
Map Network Drive...
Backup File Folder:
R:\
Browse...
Include protected data in backup set
< Back
Next >
Exit

b Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server. To perform this direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Type in the path or browse to the location to receive the backup file.

c Select an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, for example: `\\192.168.1.6\VM_BU`. Verify that the mapped partition has enough free space, a minimum of 2GB, to accommodate the backup file.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Configuration
Microsoft Windows Backup Configuration
Map Network Drive
Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Q:
Folder:
\\192.168.1.6\VM_BU
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel
Browse...
vmware
< Back
Next >
Exit

d Where the VMware Channel connection is slower than 10 Mbit/s or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

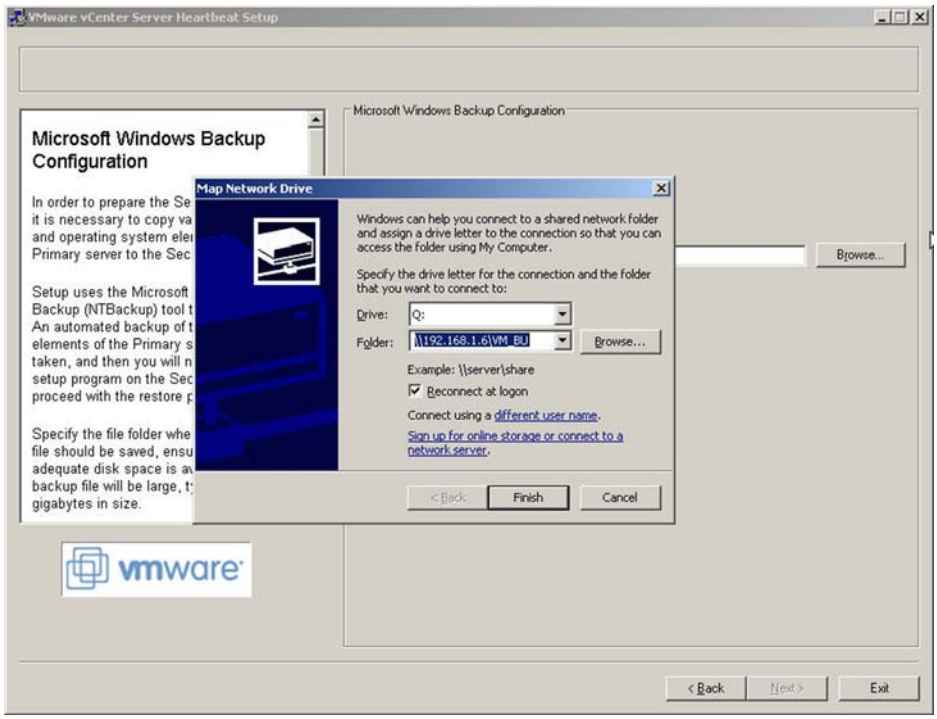
e In either scenario, specify the path to an appropriate location for storing the backup file by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping.

23 When Pre-Clone technique is selected, Setup backs up two small files, nfsetup.dat and primary.csv, from the Primary server and restores them to the Secondary server for proper configuration.

Continue with Step a.

a Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server. To perform this direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Type the path or browse to the location to receive the backup file.

b Select an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, for example: `\\192.168.1.6\VM_BU`.

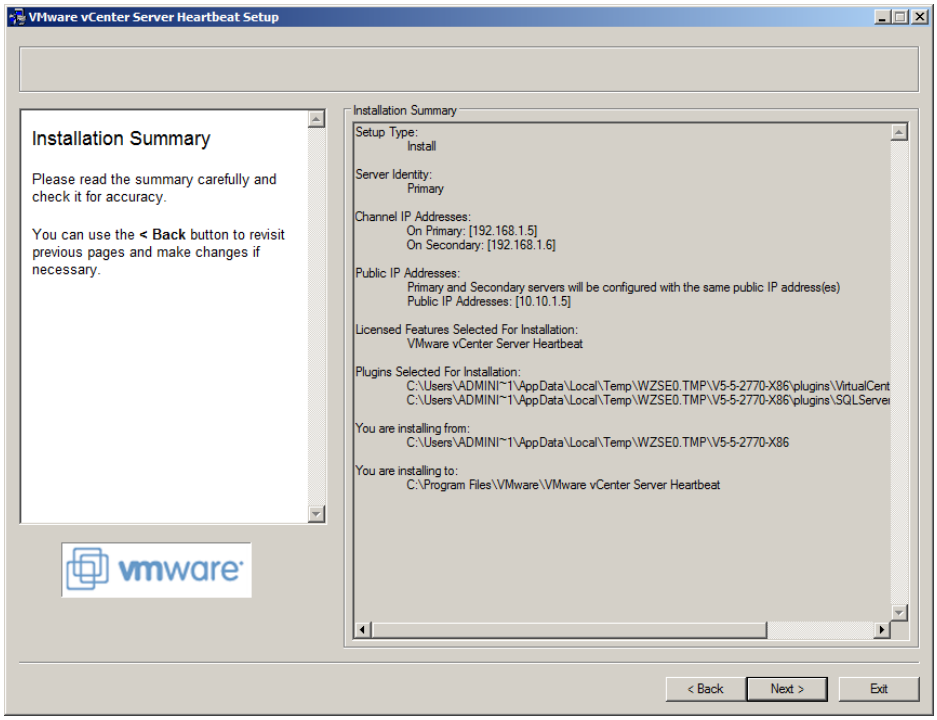

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Configuration
Microsoft Windows Backup Configuration
Map Network Drive
Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Q:
Folder:
\\192.168.1.6\VM_BU
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel
Browse...
vmware
< Back
Next >
Exit

c Where the VMware Channel connection is slower than 10 Mbit/s or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

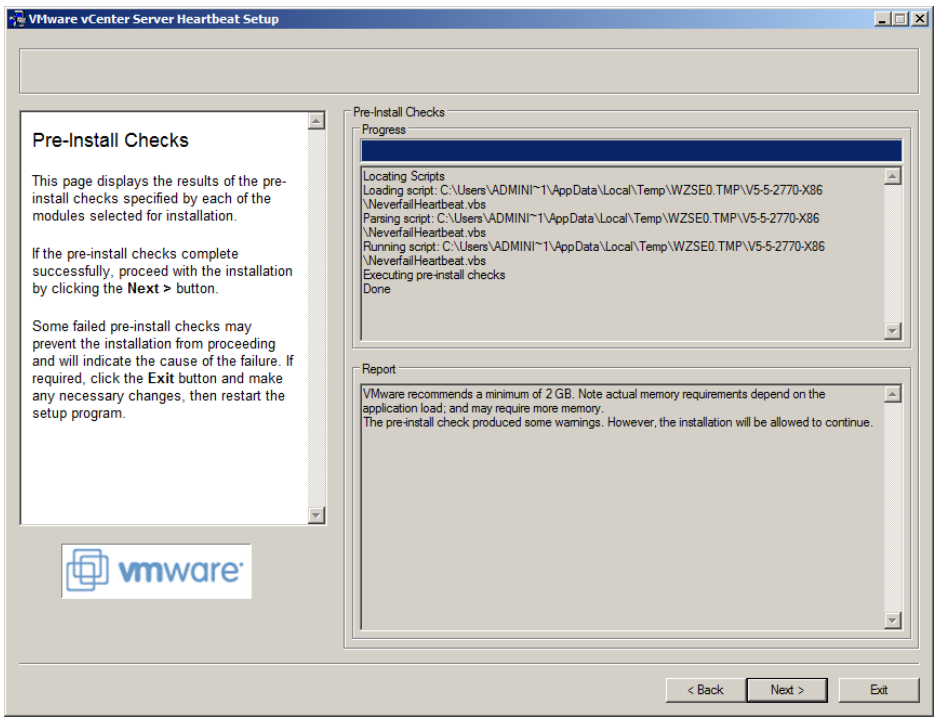
d In either scenario, specify the path to an appropriate location for storing the backup file by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping.

With Windows 2003, vCenter Server Heartbeat takes the backup using the Windows Volume Shadow Service and does not stop services, thereby preventing downtime. Click **Next**.

24 Review the summary of options and configuration information for the installation. Click **Next**.



25 Pre-install checks run to ensure that the installation can continue. Setup checks the available disk space, system memory, operating system compatibility, and dependencies between modules. The Report panel displays the results of the pre-install checks.


VMware vCenter Server Heartbeat Setup
Pre-Install Checks
This page displays the results of the pre-install checks specified by each of the modules selected for installation.
If the pre-install checks complete successfully, proceed with the installation by clicking the Next > button.
Some failed pre-install checks may prevent the installation from proceeding and will indicate the cause of the failure. If required, click the Exit button and make any necessary changes, then restart the setup program.
Pre-Install Checks
Progress
Locating Scripts
Loading script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Parsing script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Running script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Executing pre-install checks
Done
Report
VMware recommends a minimum of 2 GB. Note actual memory requirements depend on the application load; and may require more memory.
The pre-install check produced some warnings. However, the installation will be allowed to continue.
vmware
< Back
Next >
Exit

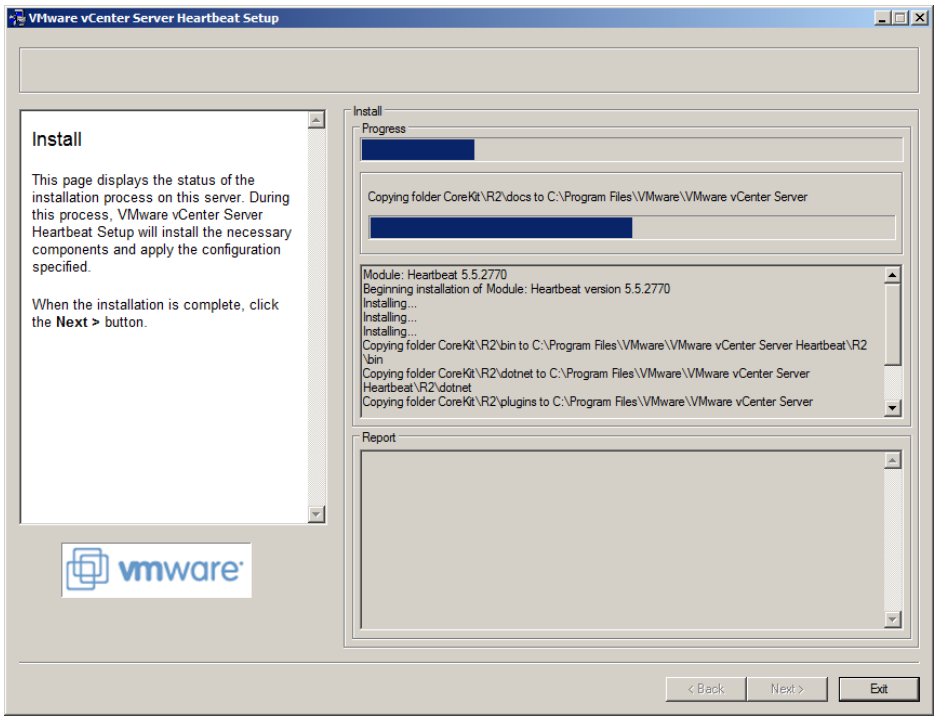
26 If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again. If the pre-install checks are successful, click **Next**.

NOTE The Progress panel on the **Pre-Install Checks** page displays the progress of these checks. When finished, the Report panel displays the results.

---

27 The next page displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and configures it with the default settings.

NOTE If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version. To learn more about Heartbeat Diagnostics, see *Getting Started with Heartbeat Diagnostics* on the VMware Web site.

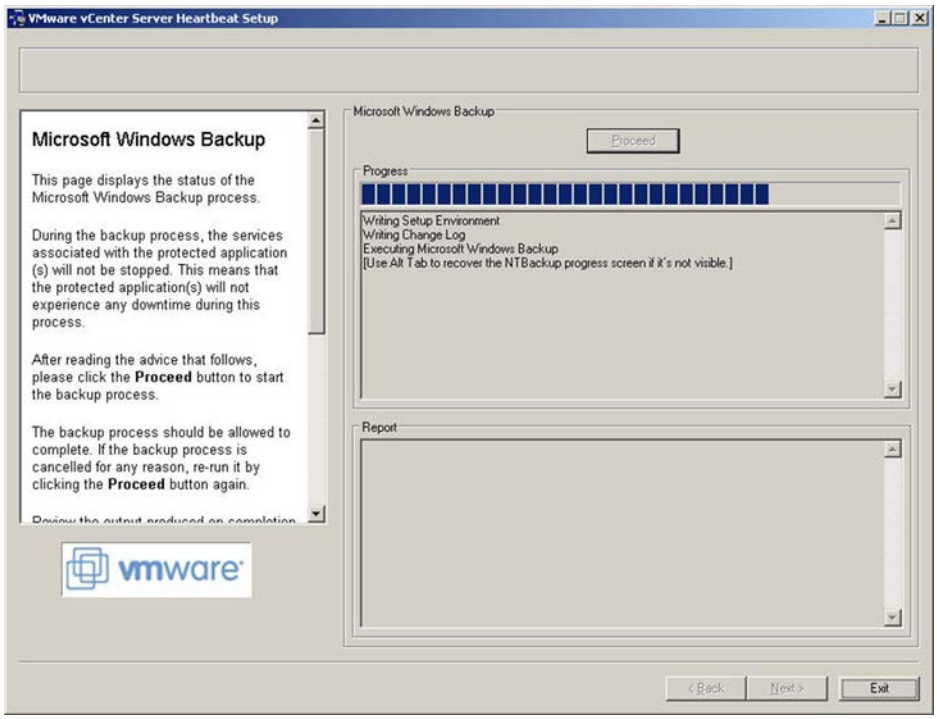

VMware vCenter Server Heartbeat Setup
Install
This page displays the status of the installation process on this server. During this process, VMware vCenter Server Heartbeat Setup will install the necessary components and apply the configuration specified.
When the installation is complete, click the Next > button.
vmware
Install
Progress
Copying folder CoreKit\R2\docs to C:\Program Files\VMware\VMware vCenter Server
Module: Heartbeat 5.5.2770
Beginning installation of Module: Heartbeat version 5.5.2770
Installing...
Installing...
Installing...
Copying folder CoreKit\R2\bin to C:\Program Files\VMware\VMware vCenter Server Heartbeat\R2\bin
Copying folder CoreKit\R2\dotnet to C:\Program Files\VMware\VMware vCenter Server Heartbeat\R2\dotnet
Copying folder CoreKit\R2\plugins to C:\Program Files\VMware\VMware vCenter Server
Report
< Back
Next >
Exit

28 Click **Next** after vCenter Server Heartbeat components are complete.

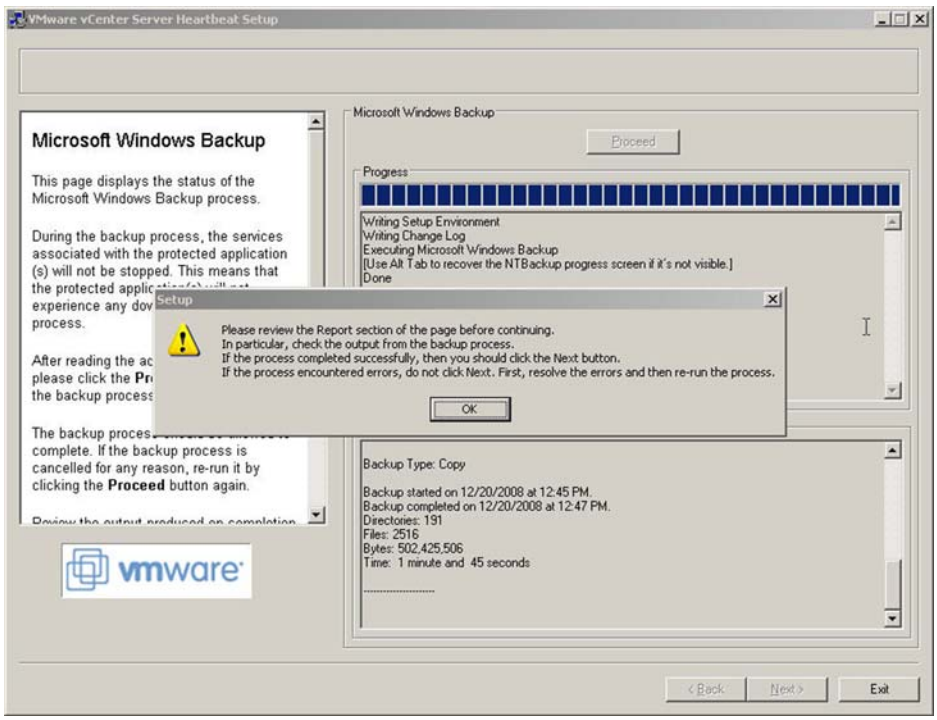
You have the following options:

- If using the Pre-Clone installation technique, go to Step 31.
- If using the Install Clone installation technique, continue to Step 29.

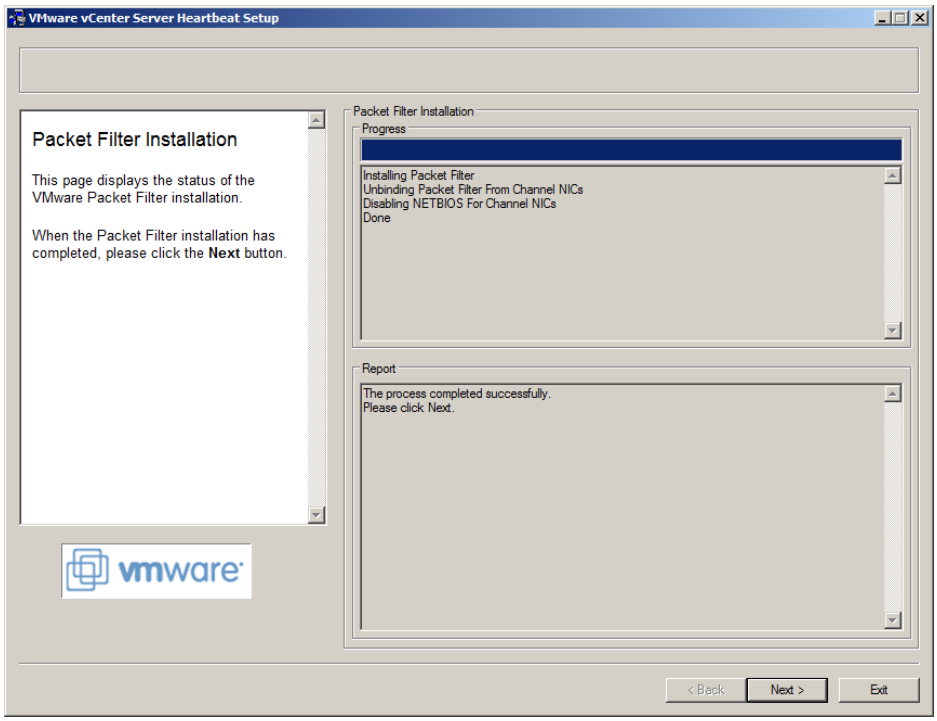
29 The next page displays the Microsoft Windows Backup panel. Click **Proceed**. The automated backup is saved in the previously defined location.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup
This page displays the status of the Microsoft Windows Backup process.
During the backup process, the services associated with the protected application (s) will not be stopped. This means that the protected application(s) will not experience any downtime during this process.
After reading the advice that follows, please click the Proceed button to start the backup process.
The backup process should be allowed to complete. If the backup process is cancelled for any reason, re-run it by clicking the Proceed button again.
Microsoft Windows Backup
Proceed
Progress
Writing Setup Environment
Writing Change Log
Executing Microsoft Windows Backup
[Use Alt Tab to recover the NTBackup progress screen if it's not visible.]
Report
vmware
< Back
Next >
Exit

30 A summary window displays the results of the backup operation. Review the backup report and click **Next**.

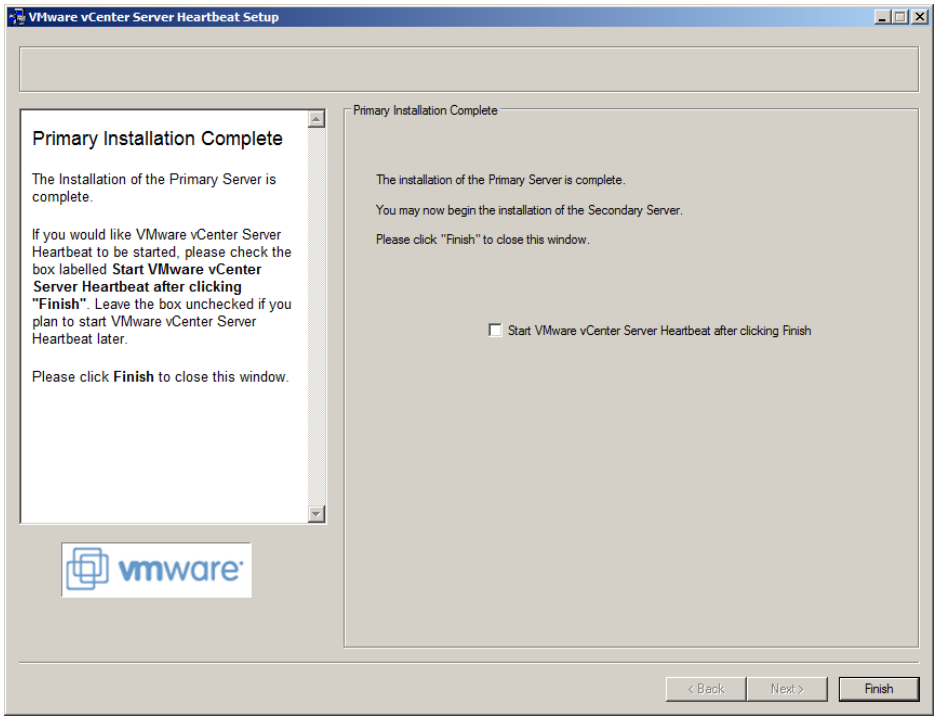

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup
This page displays the status of the Microsoft Windows Backup process.
Microsoft Windows Backup
Proceed
Progress
Writing Setup Environment
Writing Change Log
Executing Microsoft Windows Backup
[Use Alt Tab to recover the NTBackup progress screen if it's not visible.]
Done
Setup
Please review the Report section of the page before continuing.
In particular, check the output from the backup process.
If the process completed successfully, then you should click the Next button.
If the process encountered errors, do not click Next. First, resolve the errors and then re-run the process.
OK
Backup Type: Copy
Backup started on 12/20/2008 at 12:45 PM.
Backup completed on 12/20/2008 at 12:47 PM.
Directories: 191
Files: 2516
Bytes: 502,425,506
Time: 1 minute and 45 seconds
vmware
< Back
Next >
Exit

31 The vCenter Server Heartbeat Packet Filter driver installs on each network card of the production server. If you see warnings that the driver is unsigned or did not complete the Windows Logo tests, click **Continue Anyway**. If Windows is configured to display Signed Driver warnings, you can see multiple warnings. The Report panel displays the results. Click **Next**.


VMware vCenter Server Heartbeat Setup
Packet Filter Installation
This page displays the status of the VMware Packet Filter installation.
When the Packet Filter installation has completed, please click the Next button.
vmware
Packet Filter Installation
Progress
Installing Packet Filter
Unbinding Packet Filter From Channel NICs
Disabling NETBIOS For Channel NICs
Done
Report
The process completed successfully.
Please click Next.
< Back
Next >
Exit

By default, the vCenter Server Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The vCenter Server Heartbeat Packet Filter is not applied to the network cards forming VMware Channel connections as these cards maintain unique IP addresses irrespective of the role of the server. vCenter Server Heartbeat also disables NetBIOS on the Channel NIC(s) to prevent domain name conflicts on the subnet.

32 When the setup wizard confirms the successful completion of the installation, click **Finish**.

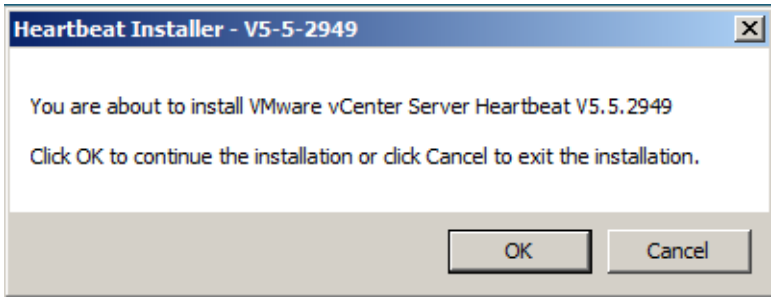

VMware vCenter Server Heartbeat Setup
Primary Installation Complete
The Installation of the Primary Server is complete.
If you would like VMware vCenter Server Heartbeat to be started, please check the box labelled Start VMware vCenter Server Heartbeat after clicking "Finish". Leave the box unchecked if you plan to start VMware vCenter Server Heartbeat later.
Please click Finish to close this window.
vmware
Primary Installation Complete
The installation of the Primary Server is complete.
You may now begin the installation of the Secondary Server.
Please click "Finish" to close this window.
Start VMware vCenter Server Heartbeat after clicking Finish
< Back
Next >
Finish

Secondary Server

The process of installing vCenter Server Heartbeat on the Secondary server is similar to installing vCenter Server Heartbeat on the Primary server.

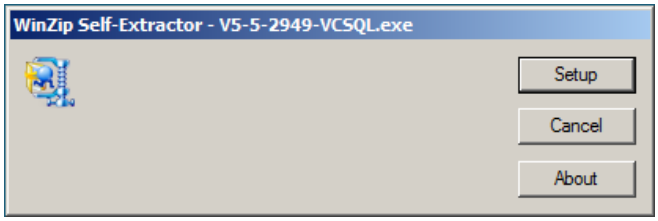
To install the Secondary server

1 To install the vCenter Server Heartbeat on the Secondary server, download vCenter Server Heartbeat to the Secondary server (either Physical or Virtual) to a suitable location. Execute the WinZip self extracting file to start the installation process. The **Setup Introduction** window appears. Review the information and click **OK**.

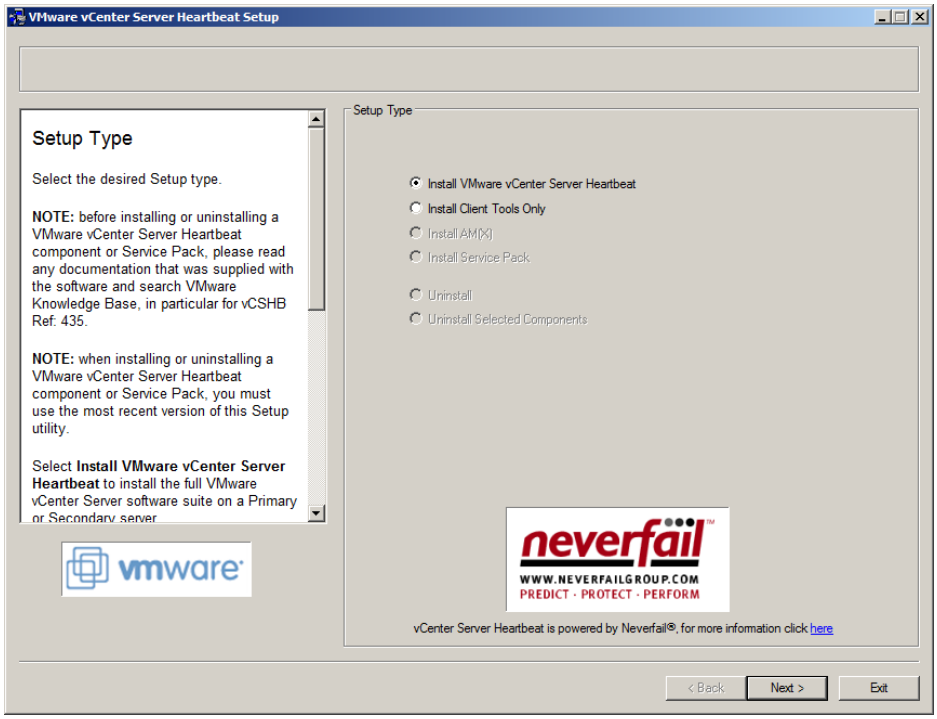

Heartbeat Installer - V5-5-2949
You are about to install VMware vCenter Server Heartbeat V5.5.2949
Click OK to continue the installation or click Cancel to exit the installation.
OK
Cancel

NOTE If you click **Exit** after Setup has started, you are prompted to save your settings. When you run the self extracting WinZip file again later, you will be asked if you want to use the previously saved configuration.

2 The **WinZip Self-Extractor** window appears. Click **Setup** to continue.

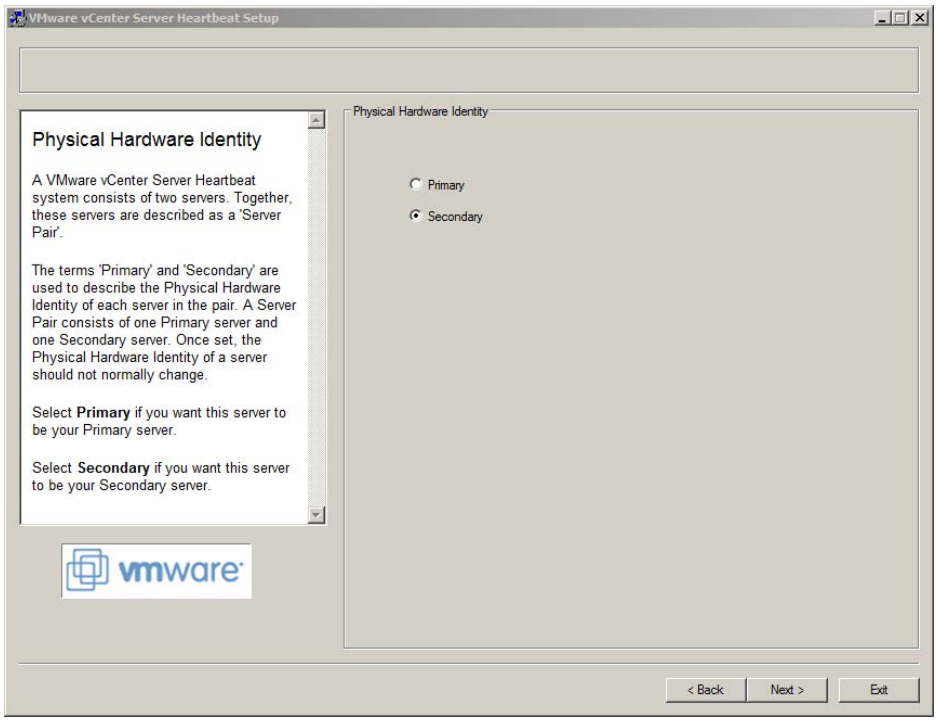


3 The **Setup Type** window appears. As with the installation on the Primary server, select **Install VMware vCenter Server Heartbeat** and click **Next**.


VMware vCenter Server Heartbeat Setup
Setup Type
Select the desired Setup type.
NOTE: before installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, please read any documentation that was supplied with the software and search VMware Knowledge Base, in particular for vCSHB Ref: 435.
NOTE: when installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, you must use the most recent version of this Setup utility.
Select Install VMware vCenter Server Heartbeat to install the full VMware vCenter Server software suite on a Primary or Secondary server
Setup Type
Install VMware vCenter Server Heartbeat
Install Client Tools Only
Install AM(X)
Install Service Pack
Uninstall
Uninstall Selected Components
neverfail
WWW.NEVERFAILGROUP.COM
PREDICT · PROTECT · PERFORM
vCenter Server Heartbeat is powered by Neverfail®, for more information click here
< Back
Next >
Exit

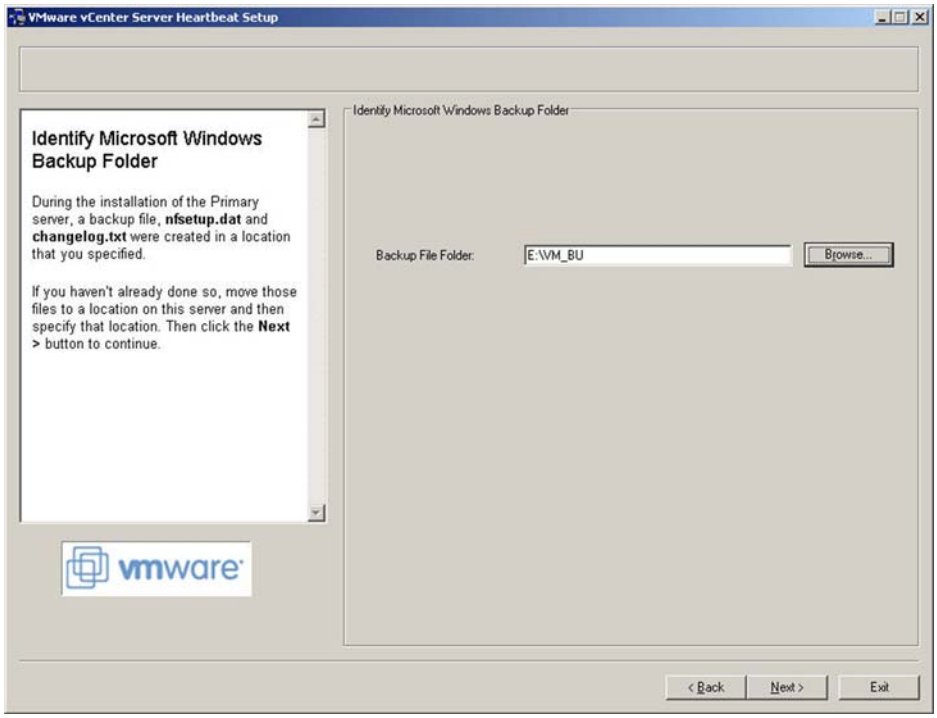
NOTE The left pane of each page in the setup wizard provides information about the setup process.

4 Select the identity of the server on the **Physical Hardware Identity** page. Select **Secondary** as the server identity and click **Next**.


VMware vCenter Server Heartbeat Setup
Physical Hardware Identity
A VMware vCenter Server Heartbeat system consists of two servers. Together, these servers are described as a 'Server Pair'.
The terms 'Primary' and 'Secondary' are used to describe the Physical Hardware Identity of each server in the pair. A Server Pair consists of one Primary server and one Secondary server. Once set, the Physical Hardware Identity of a server should not normally change.
Select Primary if you want this server to be your Primary server.
Select Secondary if you want this server to be your Secondary server.
Physical Hardware Identity
Primary
Secondary
vmware
< Back
Next >
Exit

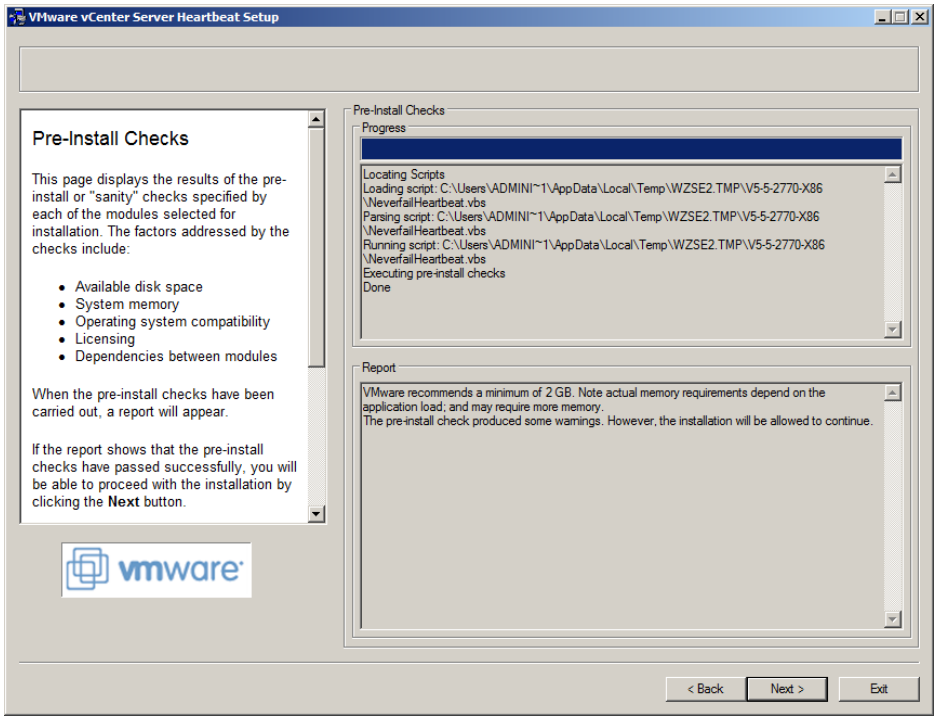
NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

5 Specify the location of the folder containing the backup file from the Primary server. Manually type the location path in the text box or click **Browse** and locate the folder. Click **Next**.


VMware vCenter Server Heartbeat Setup
Identify Microsoft Windows Backup Folder
During the installation of the Primary server, a backup file, nfsetup.dat and changelog.txt were created in a location that you specified.
If you haven't already done so, move those files to a location on this server and then specify that location. Then click the Next > button to continue.
Identify Microsoft Windows Backup Folder
Backup File Folder:
E:\VM_BU
Browse...
vmware
< Back
Next >
Exit

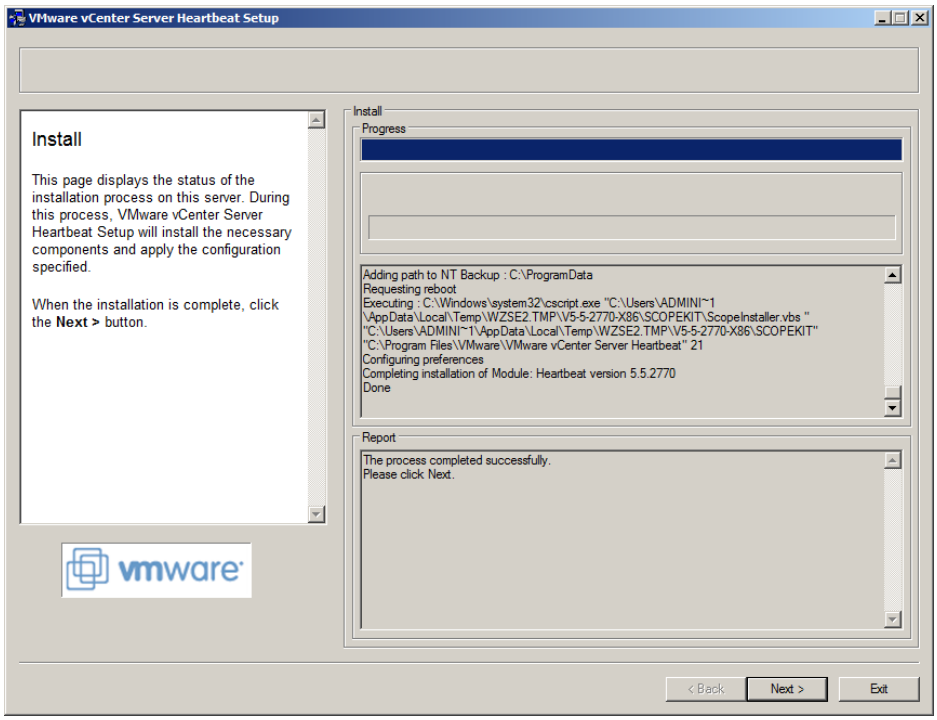
6 The pre-install checks run. Click **Next**.

If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.

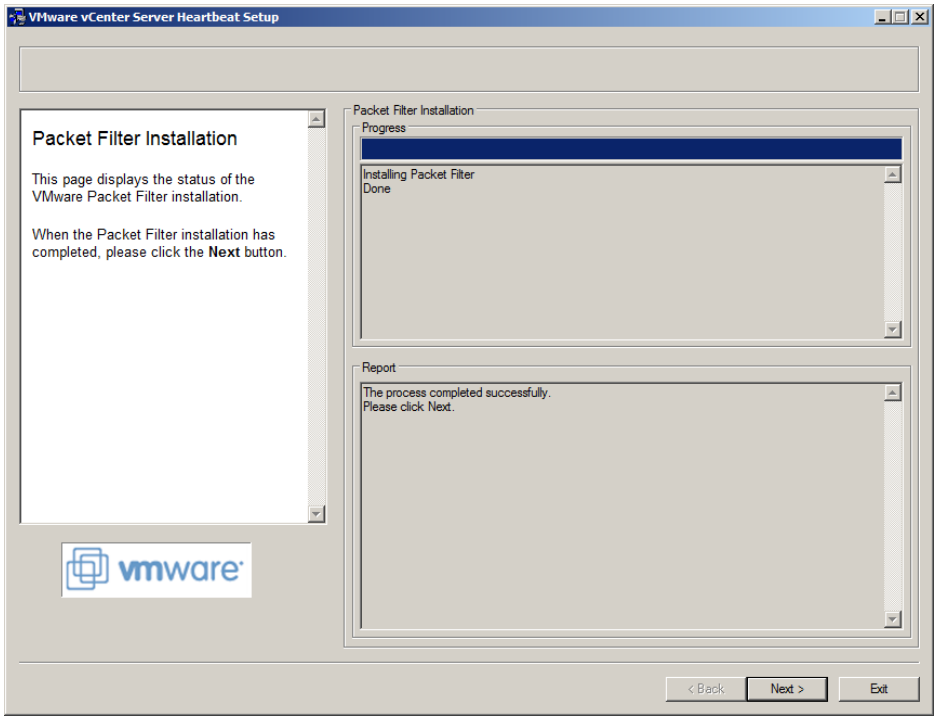

VMware vCenter Server Heartbeat Setup
Pre-Install Checks
This page displays the results of the pre-install or "sanity" checks specified by each of the modules selected for installation. The factors addressed by the checks include:
Available disk space
System memory
Operating system compatibility
Licensing
Dependencies between modules
When the pre-install checks have been carried out, a report will appear.
If the report shows that the pre-install checks have passed successfully, you will be able to proceed with the installation by clicking the Next button.
vmware
Pre-Install Checks
Progress
Locating Scripts
Loading script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Parsing script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Running script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Executing pre-install checks
Done
Report
VMware recommends a minimum of 2 GB. Note actual memory requirements depend on the application load; and may require more memory.
The pre-install check produced some warnings. However, the installation will be allowed to continue.
< Back
Next >
Exit

7 The next page displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and configures it with the default settings. To learn more about Heartbeat Diagnostics see *Getting Started with Heartbeat Diagnostics*.

8 The Report panel displays the results of the installation. Click **Next**.


VMware vCenter Server Heartbeat Setup
Install
This page displays the status of the installation process on this server. During this process, VMware vCenter Server Heartbeat Setup will install the necessary components and apply the configuration specified.
When the installation is complete, click the Next > button.
vmware
Install
Progress
Adding path to NT Backup : C:\ProgramData
Requesting reboot
Executing : C:\Windows\system32\cscript.exe "C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\SCOPEKIT\ScopeInstaller.vbs " "C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\SCOPEKIT" "C:\Program Files\VMware\VMware vCenter Server Heartbeat" 21
Configuring preferences
Completing installation of Module: Heartbeat version 5.5.2770
Done
Report
The process completed successfully.
Please click Next.
< Back
Next >
Exit

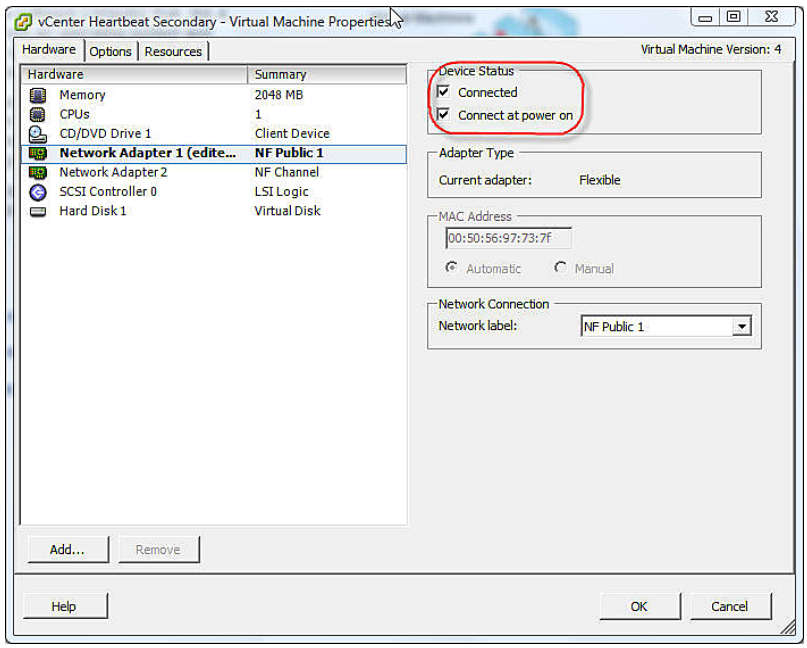
9 The progress of the VMware vCenter Server Heartbeat Packet Filter installation is displayed. Click **Next**.



You have the following options:

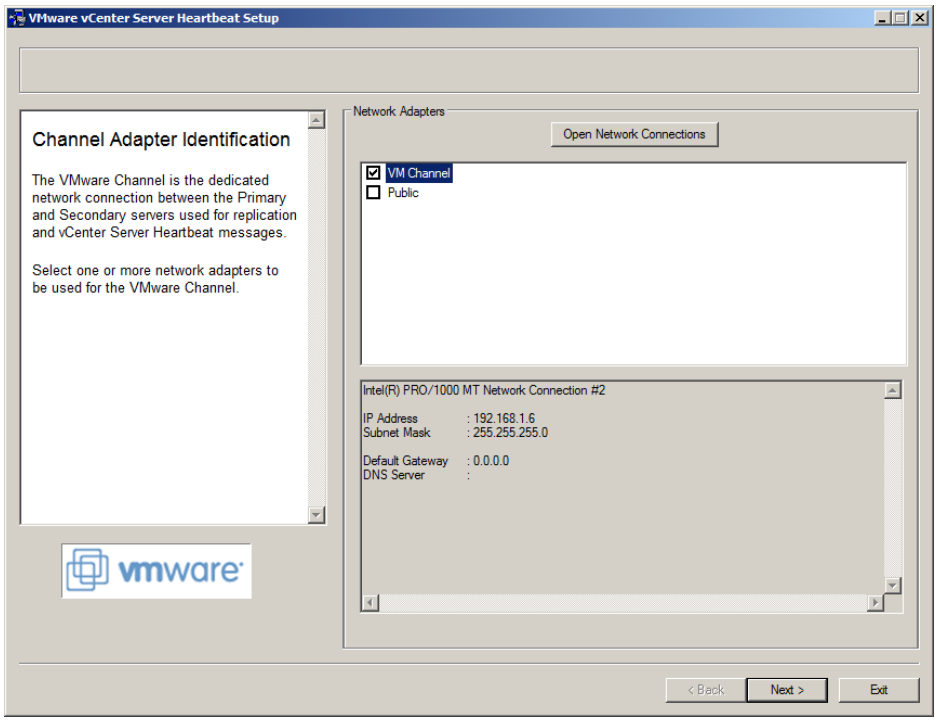
- If the Secondary server is physical, such as in P2P, go to Step 10.
- If the Secondary server is virtual, such as in P2V or V2V, continue with Step a.

a The Packet Filter is installed on the Principal (Public) NIC and the Principal (Public) network adapter can be reconnected. Right-click the Secondary server image name and select **Edit Settings**.



b Select the Principal (Public) virtual network adapter, select the **Connected** and **Connect at power on** check boxes, and click **OK**.

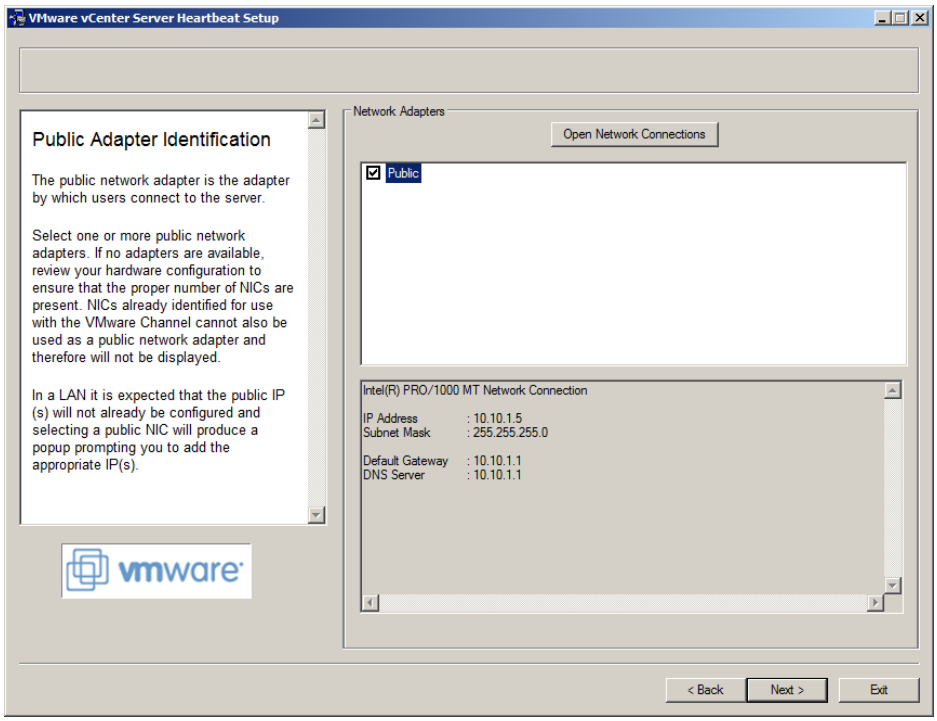
10 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower panel. Click **Next**.


VMware vCenter Server Heartbeat Setup
Channel Adapter Identification
The VMware Channel is the dedicated network connection between the Primary and Secondary servers used for replication and vCenter Server Heartbeat messages.
Select one or more network adapters to be used for the VMware Channel.
vmware
Network Adapters
Open Network Connections
VM Channel
Public
Intel(R) PRO/1000 MT Network Connection #2
IP Address : 192.168.1.6
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
DNS Server :
< Back
Next >
Exit

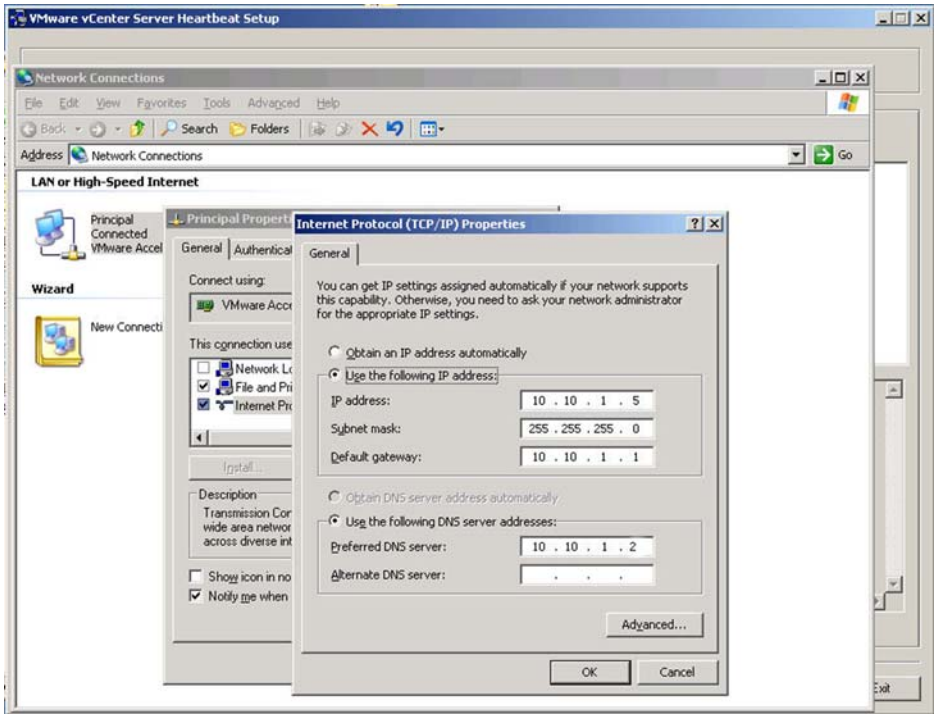
You have the following options:

- If using the Install Clone installation technique, continue to Step 11.
- If using the Pre-Clone installation technique, go to Step 14.

11 Configure the Principal (Public) adapter on the Secondary server through the **Public Adapter Identification** page. When you select the Principal (Public) adapter, a caution message notifies you that the IP address on the Principal (Public) adapter does not match the IP address on the Primary server (LAN configuration only). Click **OK**.


VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
In a LAN it is expected that the public IP (s) will not already be configured and selecting a public NIC will produce a popup prompting you to add the appropriate IP(s).
vmware
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
< Back
Next >
Exit

12 Click **Open Network Connections** to change the static IP address of the Principal (Public) adapter to match that of the Primary server (LAN configuration only).

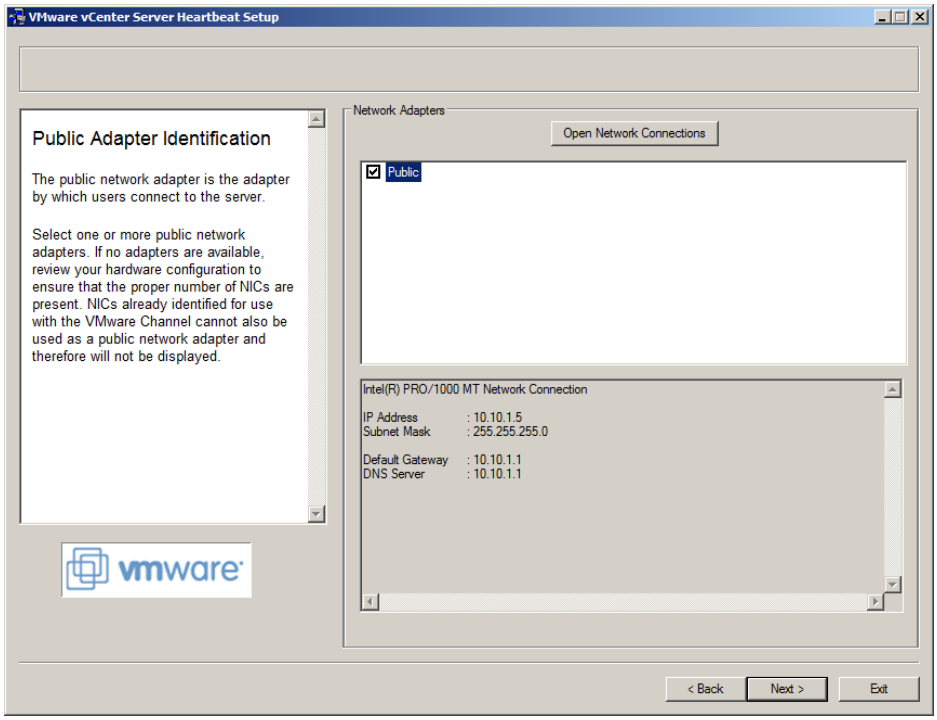

VMware vCenter Server Heartbeat Setup
Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
LAN or High-Speed Internet
Principal Connected VMware Accel
Wizard
New Connecti
Principal Properti
General Authentica
Connect using:
VMware Acc
This connection use
Network Lo
File and Pri
Internet Pr
Install...
Description
Transmission Cor wide area networ across diverse int
Show icon in no
Notify me when
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 1 . 5
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 1 . 2
Alternate DNS server:
Advanced...
OK
Cancel
Exit

13 If in a WAN environment, verify the Secondary Principal (Public) adapter IP address configuration. Click **Next**.

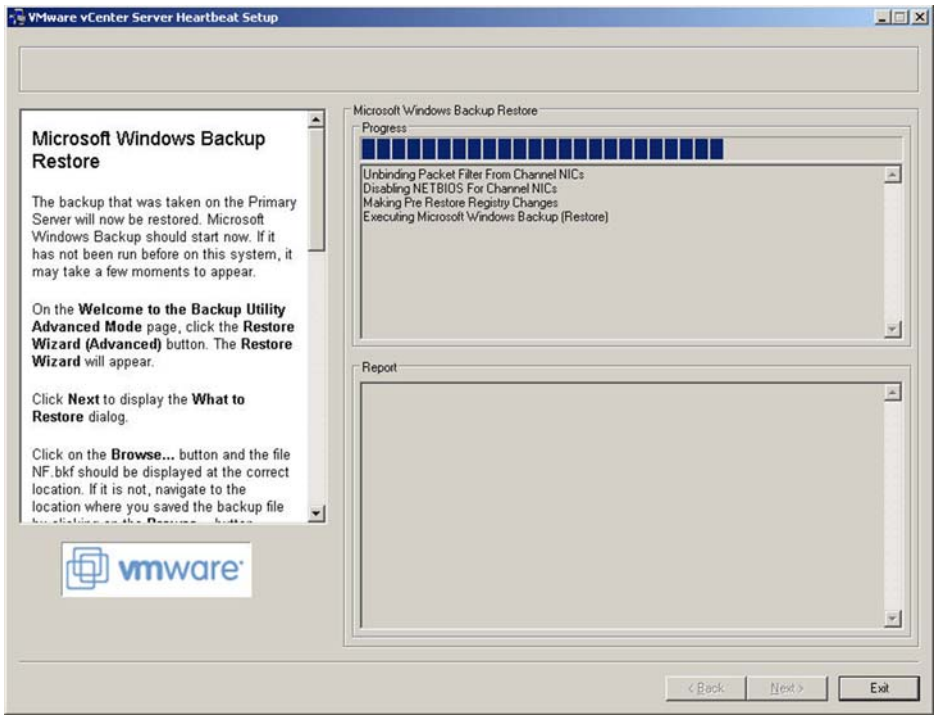
You have the following options:

- If using the Install Clone installation technique, go to Step 15.
- If using the Pre-Clone installation technique, go to Step 28.

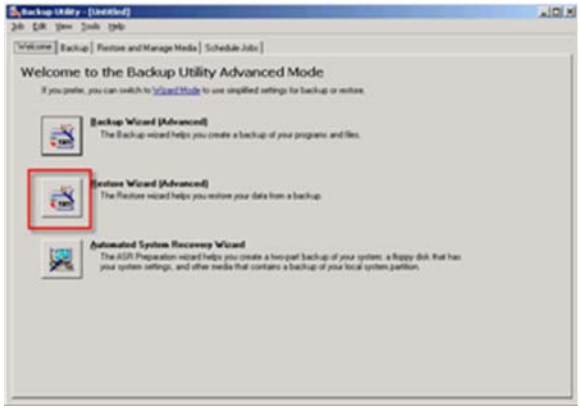
14 When using the Pre-Clone installation technique, although you previously configured the IP address of the Principal (Public) network connections, you can make any last minute changes on the Secondary server through vCenter Server Heartbeat. Click **Next**.


VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
vmware
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
< Back
Next >
Exit

15 The **Microsoft Windows Backup Restore** page shows the process of unbinding the vCenter Server Heartbeat Packet Filter and disabling NetBIOS from the VMware Channel NIC(s). A caution message appears, advising you that the restore process is initiating and upon completion, the server must be restarted. After restarting, Plug and Play (PnP) can require you to restart the machine again. Click **Next**.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Restore
The backup that was taken on the Primary Server will now be restored. Microsoft Windows Backup should start now. If it has not been run before on this system, it may take a few moments to appear.
On the Welcome to the Backup Utility Advanced Mode page, click the Restore Wizard (Advanced) button. The Restore Wizard will appear.
Click Next to display the What to Restore dialog.
Click on the Browse... button and the file NF.bkf should be displayed at the correct location. If it is not, navigate to the location where you saved the backup file
vmware
Microsoft Windows Backup Restore
Progress
Unbinding Packet Filter From Channel NICs
Disabling NETBIOS For Channel NICs
Making Pre Restore Registry Changes
Executing Microsoft Windows Backup (Restore)
Report
< Back
Next >
Exit

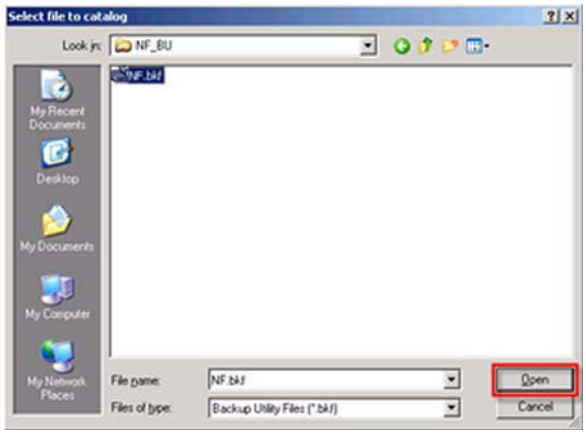
16 The NTBackup wizard launches. If NTBackup has never run before, the software searches for backup devices. Close any open wizards and click **Restore Wizard** on the welcome page.



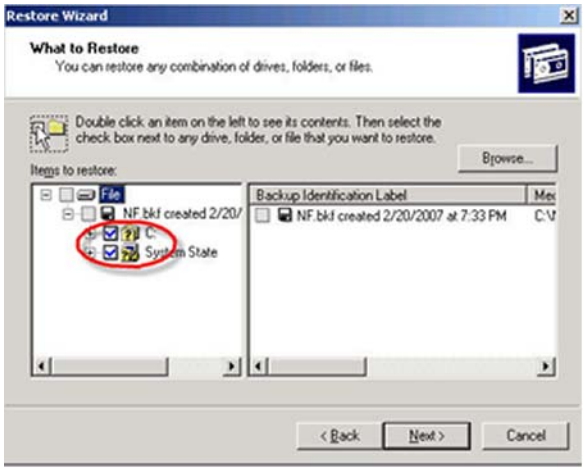
17 Click **Next** in the Restore Wizard. Click **Browse** to locate the previously generated backup file.

Restore Wizard
What to Restore
You can restore any combination of drives, folders, or files.
Double click an item on the left to see its contents. Then select the check box next to any drive, folder, or file that you want to restore.
Browse...
Items to restore:
File
Backup Identification Label
No entries found.

18 Navigate to the partition and select the folder in which the backup file was created, select the backup file, click **Open** and then click **OK**.



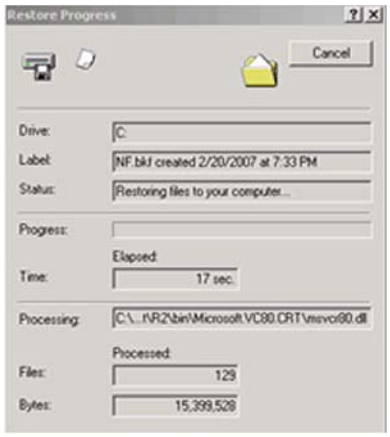
19 Expand the file tree structure to see the System State file in the left panel. Click **OK** to build indexes where required. Select all items listed under the media created tree and click **Next**.


Restore Wizard
What to Restore
You can restore any combination of drives, folders, or files.
Double click an item on the left to see its contents. Then select the check box next to any drive, folder, or file that you want to restore.
Browse...
Items to restore:
File
NF.bkf created 2/20/
C:
System State
Backup Identification Label
NF.bkf created 2/20/2007 at 7:33 PM
< Back
Next >
Cancel

20 With **Where to restore** at the default **Original location**, click **Next**. Click **Finish**.

Restore Wizard
Completing the Restore Wizard
You have successfully completed the Restore wizard. You specified the following settings:
Restore from: File
Media: Multiple media
Restore to: Original locations
Existing files: Always replace
To close this wizard and start the restore, click Finish.
To specify additional options, click Advanced.
Advanced...
< Back
Finish
Cancel

21 A warning message alerts you that the restore process is going to overwrite the existing System State files. Click **OK** to allow the restore process to continue.



22 When the restoration process completes, click **Close**.

23 To apply the newly restored system state, you must restart the machine. Click **Yes** to restart the server.

24 Following the restart of the server, log in to the Secondary server using a domain administrator account.

25 PnP can require multiple restarts of the server as it reidentifies the actual hardware makeup of the Secondary server as opposed to that restored from the backup file of the Primary server.

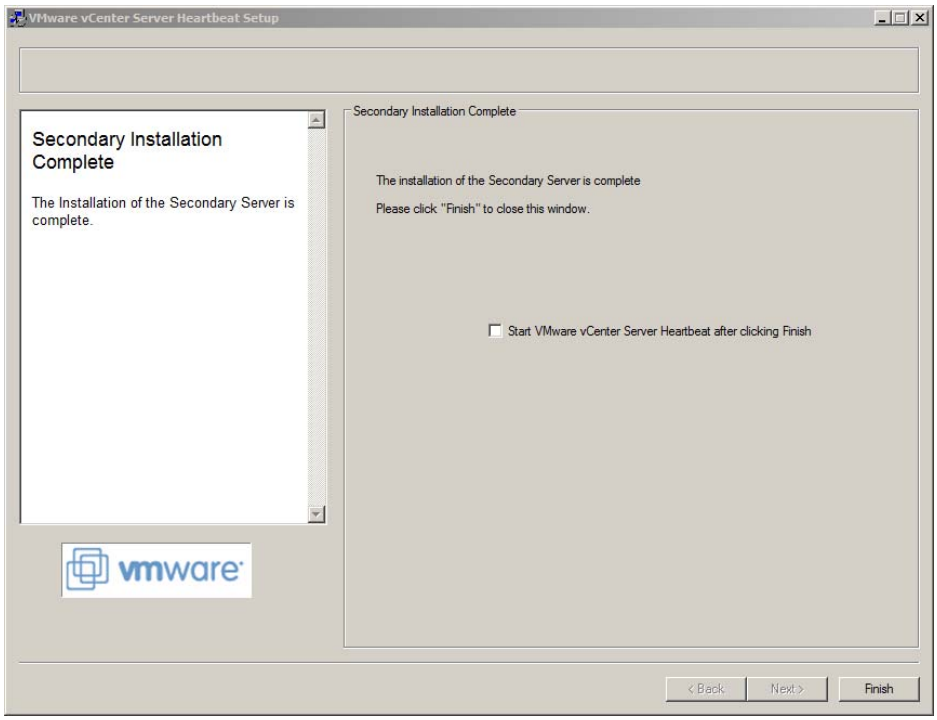
NOTE vCenter Server Heartbeat starts each time the Secondary server restarts. Manually shut down vCenter Server Heartbeat before initiating a restart.

---

26 Click **Yes** at each restart prompt to allow each PnP cycle to complete.

27 When all PnP cycles complete, the vCenter Server Heartbeat Setup is complete, and vCenter Server Heartbeat starts on the Secondary server.

28 Select **Start VMware vCenter Server Heartbeat after clicking Finish** and click **Finish**.


VMware vCenter Server Heartbeat Setup
Secondary Installation Complete
The Installation of the Secondary Server is complete.
Secondary Installation Complete
The installation of the Secondary Server is complete
Please click "Finish" to close this window.
Start VMware vCenter Server Heartbeat after clicking Finish
vmware
< Back
Next >
Finish

29 Before starting vCenter Server Heartbeat, verify the time synchronization between the Primary and Secondary servers. When a difference exists, synchronize the Secondary (passive) server to the Primary (active) server across the VMware Channel. Type the following command at the command prompt:

```
net time \\<Primary_Channel_IP_address> /set
```

Start vCenter Server Heartbeat on the Primary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icons change from a double dash to a **P** indicating the server is the Primary server, and an **A** indicating the server is acting in an active role.

30 The Primary and Secondary servers establish a handshake and commence replication.

NOTE The installation is complete if vCenter Server was installed with a local SQL Server or only vCenter Server was installed with no separate SQL Server.

If vCenter Server only was installed and you want to install a separate SQL Server, repeat the installation process for the Primary and Secondary server at the remote site and selecting **SQL Server only**.

To install the SQL Server on a separate host from the vCenter Server, go to "Primary Server" on page 32.

31 Configure the appropriate username and password in the vCenter Server Heartbeat Console:

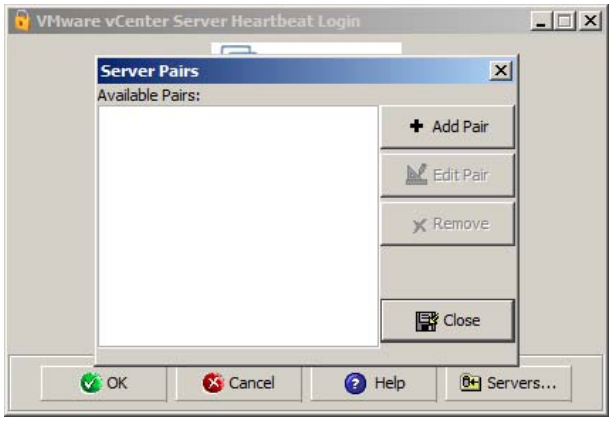
a Start vCenter Server Heartbeat Console from the desktop shortcut or **Start** > **All Programs** > **VMware** > **VMware vCenter Server Heartbeat** > **Manage Server**. The login window appears.

b Before you log in, you must identify the pair of servers to administer. Click **Servers**.

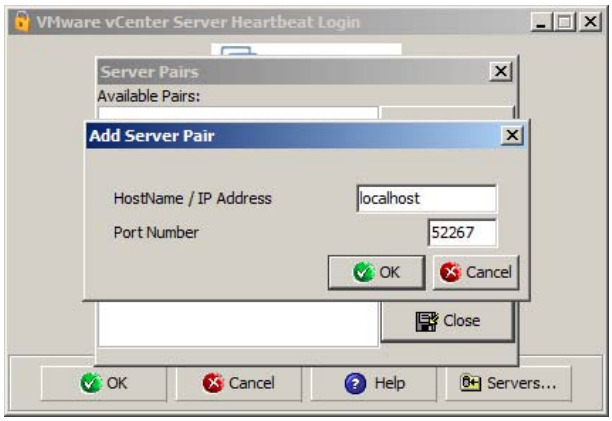
NOTE Add the Principal (Public) IP address or FQDN of the Primary server to ensure that you can administer the server pairs from the vCenter Server Heartbeat Console regardless of the role (active or passive) of the current server.

---

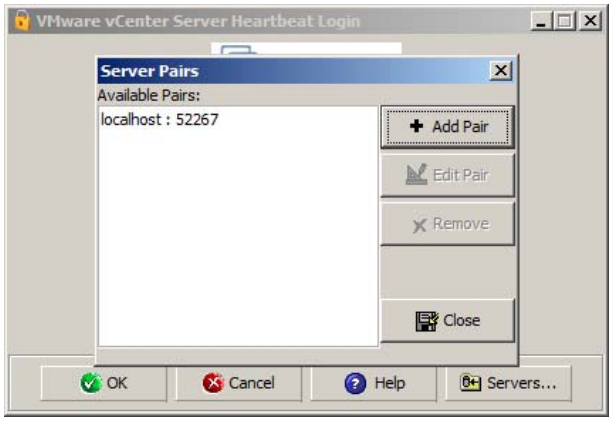
c Click **Add Pair**.



d Type the IP address of any NIC on the active server or the NetBIOS name of the server pair and click **OK**.



e The server pair appears in the list. If more than one server pair exists within the organization, add them sequentially to the list by repeating the procedure.

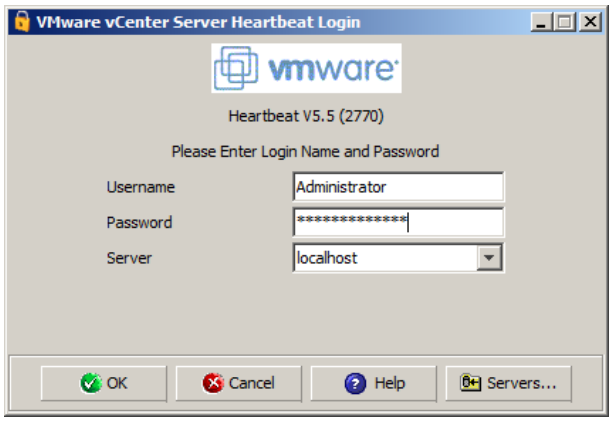


To edit or delete server pairs from the list, click the entry in the list and click the relevant button.

f Click **Close** to return to the login window.

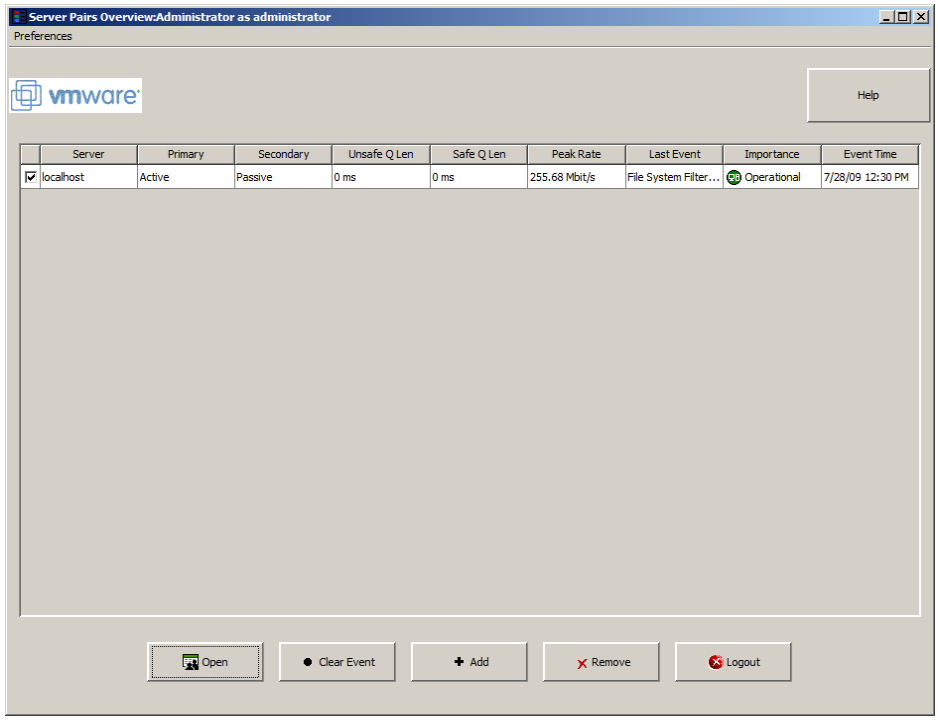
To administer a pair of servers you must connect to them through the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes. Wait 10 seconds after starting vCenter Server Heartbeat before attempting to connect.

g Select a server pair displayed in the Server box.



h Type a username and password with valid Windows credentials into the respective text boxes. In a domain environment, use the format **`domainname\username`**.

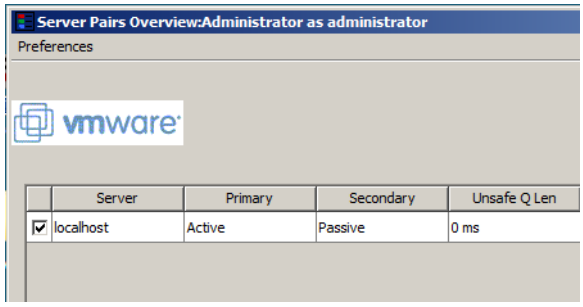
i The **Server Pairs Overview** window lists the selected pair of servers with other server pairs that historically were administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.



Additionally, the **Last Event**, **Importance**, and **Time** are displayed. These events are discussed later in this guide.

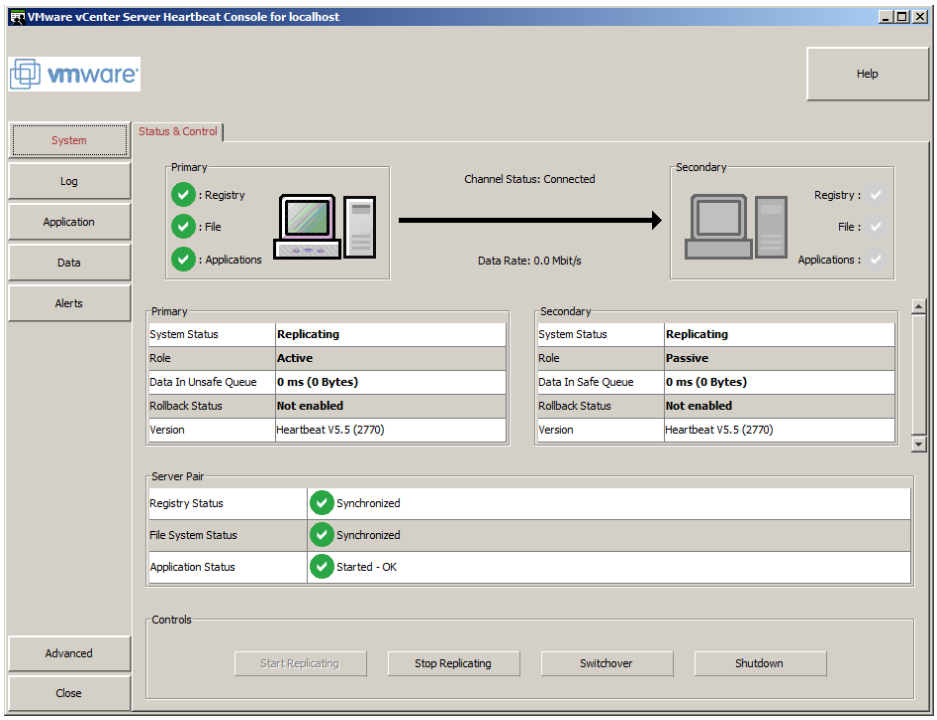
j To add additional pairs of servers, click **Add** and follow the previously described procedure.

To select a pair listed in the main data grid, select the check box next to the server name.

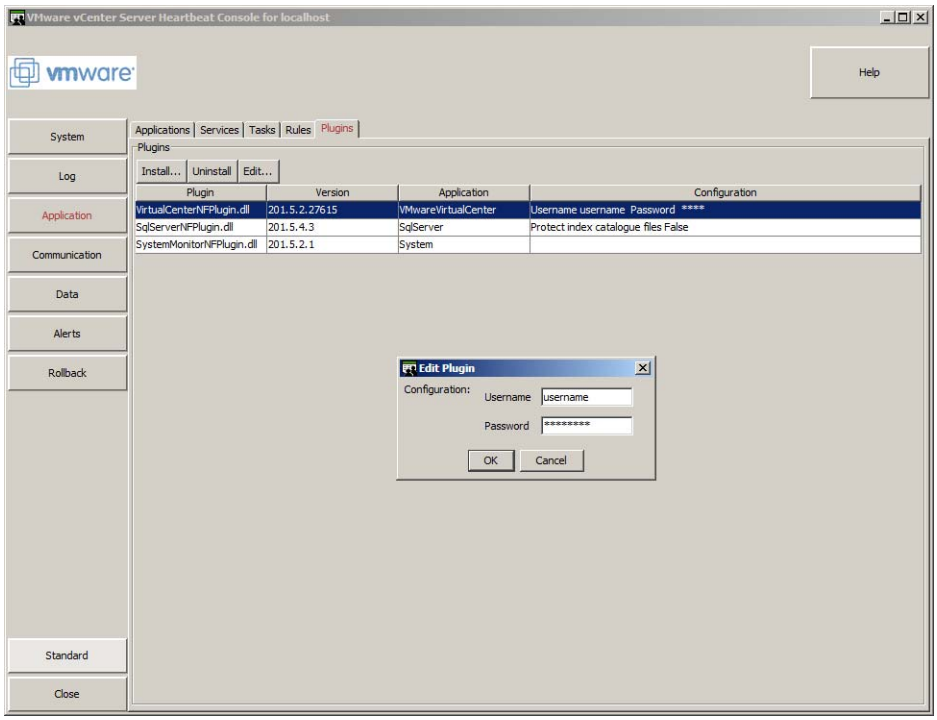


When a pair is selected, the **Open**, **Clear Event**, and **Remove** buttons become active.

Open displays the pair of servers for administration and configuration and displays the **System** > **Status and Control** page.



k Click **Advanced** > **Application** > **Plugins**.



l Select the vCenter Server plug-in.

m Click **Edit**.

n Type the **`Username`** and **`Password`** for an account with rights to the virtual infrastructure.

o Click **OK**.

Post Installation Configuration

Upon completion of installation, a series of tasks must be performed to ensure that vCenter Server Heartbeat is properly configured.

Add the VMware License

After completion of installation, vCenter Server Heartbeat will run in the evaluation mode for up to 60 days. After acquiring a license, you must add the VMware vCenter Server Heartbeat serial number using the Configure Server wizard to change from evaluation mode to production mode. To add the license:

1 Right-click the **System Tray** icon and select **Stop VMware vCenter Server Heartbeat** opting to leave protected applications running.

2 Double-click the **Configure Server** icon on the desktop.

3 Select the **License** tab of the Configure Server wizard.

4 Select the existing serial number and click the **Trash Can** icon.

5 Click the **Add Row** icon and enter the VMware vCenter Server Heartbeat serial number.

6 Click **Finish**.

7 Right-click the **System Tray** icon and select **Start VMware vCenter Server Heartbeat**.

When Deployed in a WAN Environment

When deployed in a WAN environment with VMware Orchestrator and the Primary and Secondary servers in different subnets, you must configure an Exclusion File Filter following the steps below:

1 Launch **vCenter Server Heartbeat Console**.

2 Click **Advanced** to enable Advanced mode view.

3 Click **Data** and click the **Configuration** tab.

4 Click **Add Exclusion Filter...** and type the following path:

```
$INSTALL_PATH_TO_ORCHESTRATOR/app-server/bin/boot.properties
```

5 Click **OK.**

6 Perform a switchover so that the Secondary server becomes active.

7 Launch the **vCenter Orchestrator Web Configuration** wizard and select **Network**. In the **IP address** field select the Principal (Public) IP address of the Secondary server. Click **Apply changes**.

8 Launch the **vCenter Orchestrator Web Configuration** wizard and type the Principal (Public) IP address of the Secondary server (**Network** > **IP address**).

9 Launch the **vCenter Orchestrator Web Configuration** wizard, select **Startup Options**, and click **Restart service**.

10 From **vCenter Server Heartbeat Console**, select **Application** and then **Services**. Verify that **VMware vCenter Orchestrator Server** service is included in the protected services. If not, manually run the **Protected Service Discovery** task from **VMware vCenter Heartbeat Console** > **Application** > **Tasks** > **VMware VirtualCenter - Protected Service Discovery**)

vCenter Server 2.5

The post installation configuration tasks are determined by the type of network environment.

LAN

For LAN deployments, perform the following:

1 If a Management IP address is configured, no additional tasks are required.

2 If a Management IP address is not configured, configure a VMware Managed IP address using the Virtual Infrastructure Client.

   a Launch the Virtual Infrastructure Client.

   b In the Virtual Infrastructure Client, navigate to **Administration** > **VirtualCenter Management Server Configuration** > **Runtime Settings**.

   c In the **Managed IP** field, type the Principal (Public) IP address.

   d Click **OK** and close the window.

WAN

For WAN deployments, regardless of whether a Management IP address exists, vCenter Server Heartbeat provides a task that can be configured to update the ESX hosts with the new Managed IP address during a switchover or failover. The task requires setting the Managed IP in either the `vpxd.cfg` file or in the registry.

To configure the Managed IP in the Vpxd file

1 The `vpxd.cfg` files is located at `C:\Documents and Settings\All Users\Application Data\VMware\VMware Virtual Center server`.

2 On the active server, locate the `<vpxd>` element in the `vpxd.cfg` file and add a new element `<managedIP>` that contains the Principal (Public) IP address of the vCenter server.

To configure the Managed IP in the registry

At `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VirtualCenter`, create a new string value called `<managedIP>` and set it with the Public (Principal) IP address of the currently active server.

IMPORTANT Do not configure the VMware Managed IP address using the Virtual Infrastructure Client. The Managed IP field from **Administration** > **VirtualCenter Management Server Configuration** > **Runtime Settings** must be clear.

---

vCenter Server 4.0

The post installation configuration tasks are determined by the type of network environment.

LAN

With or without a Management IP address configured, no additional tasks are required.

WAN

With or without a Management IP address configured, disable the **VMware VirtualCenter PostStart** task through the vCenter Server Heartbeat Console using the following procedure.

1 Launch the vCenter Server Heartbeat Console.

2 Click **Application**.

3 Click the **Tasks** tab.

4 Select **VMware VirtualCenter PostStart** task.

5 Click **Edit**.

6 Clear the **Enabled** check box.

7 Click **OK**.

IMPORTANT Do not configure the Managed IP address using the vSphere Client. The vCenter Server Managed IP field from **Administration** > **vCenter Server Settings** > **Runtime Settings** must be clear.

vCenter Server Heartbeat Installation on Windows Server 2008

4

This chapter includes the following topics:

- "Overview" on page 71
- "Installation Process" on page 71
- "Primary Server" on page 72
- "Secondary Server" on page 92
- "Post Installation Configuration" on page 109

Overview

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2008. During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. Should the server fail one of the checks, a critical stop or warning message is displayed. Refer to the Appendix – Setup Error Messages of this guide for a list of the checks and explanations of the messages. You must resolve critical stops before you can proceed with setup.

Prior to installing vCenter Server Heartbeat, you must identify the deployment options you want. The installation process requires you to select options throughout the procedure to achieve your configuration goals.

Installation Process

After selecting implementation options, begin the installation process. The installation process for all scenarios follows the same basic procedure. Links to specific installation scenarios describing differences are identified by the blue hyperlinked text.

Primary Server

Installation of vCenter Server Heartbeat begins on the Primary Server.

NOTE vCenter Server Heartbeat installs in the evaluation mode. Refer to "Post Installation Configuration" on page 109 for instructions on how to enter a production serial number.

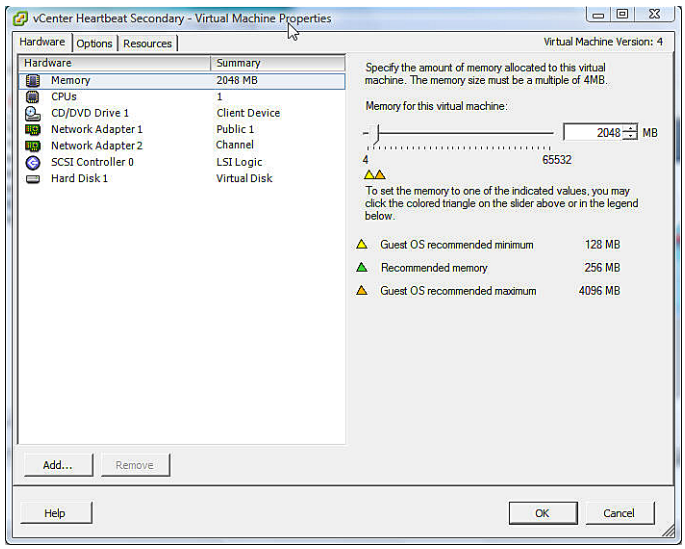
1 Having verified all of the environmental prerequisites are met, download vCenter Server Heartbeat the WinZip self extracting file to an appropriate location on the Primary server (either Physical or Virtual).

You have the following options:

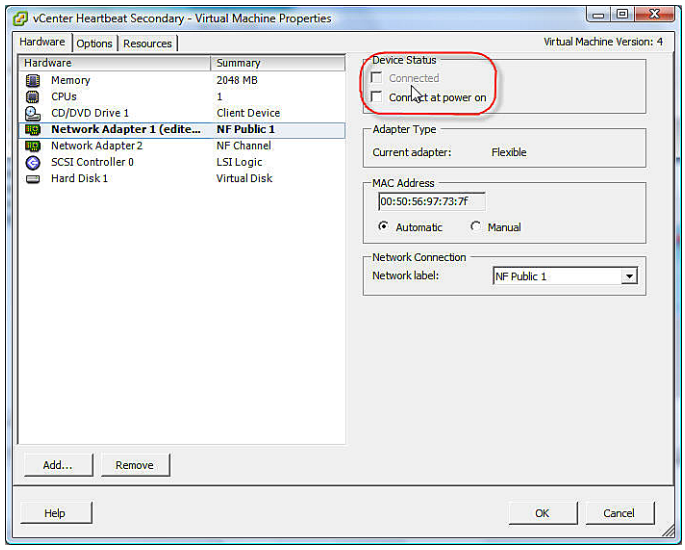
- For P2P, go to Step 2 to continue the installation.
- For V2V or P2V Installations with the Pre-Clone technique selected, begin with Step a below to configure the network settings on the Secondary server.

a Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third-party utility to create a cloned image of the Primary server. The clone must be completely identical with no changes to the Name, SID, or domain membership.

b After the cloned image is created, but before powering on the cloned image, edit the image settings.



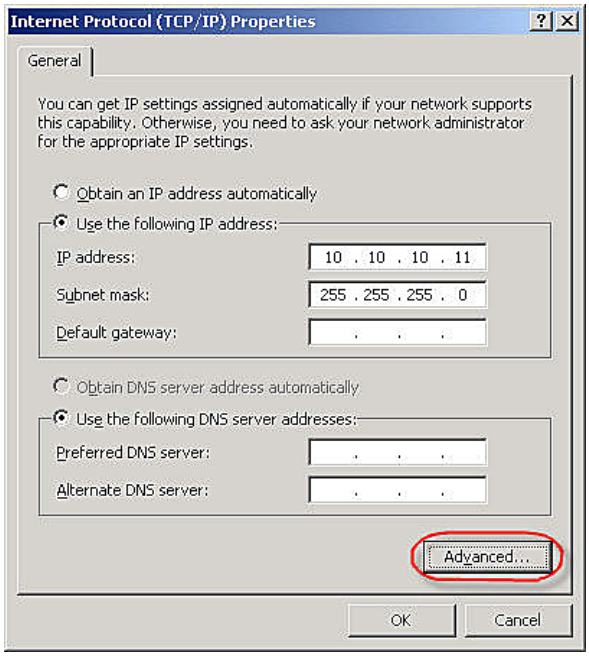
c Select the Public virtual network adapter and clear the **Connected** and **Connect at power on** check boxes.



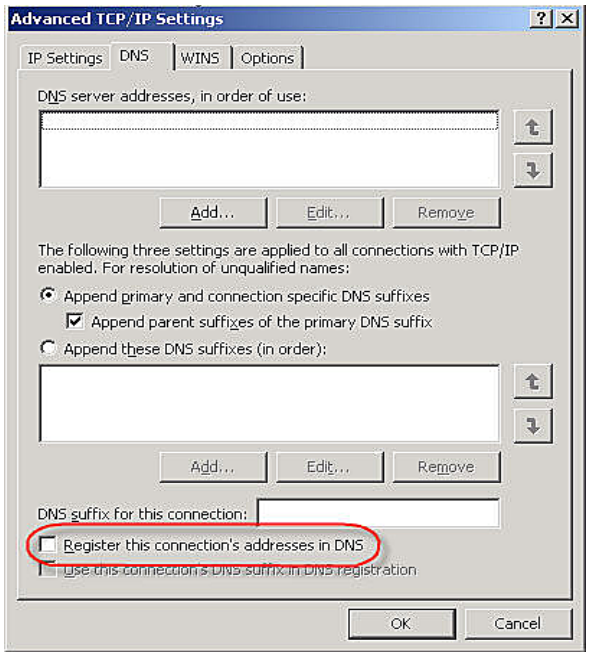
d Repeat the process on the Channel virtual network Adapter.

e Power on the Secondary (previously cloned) server image.

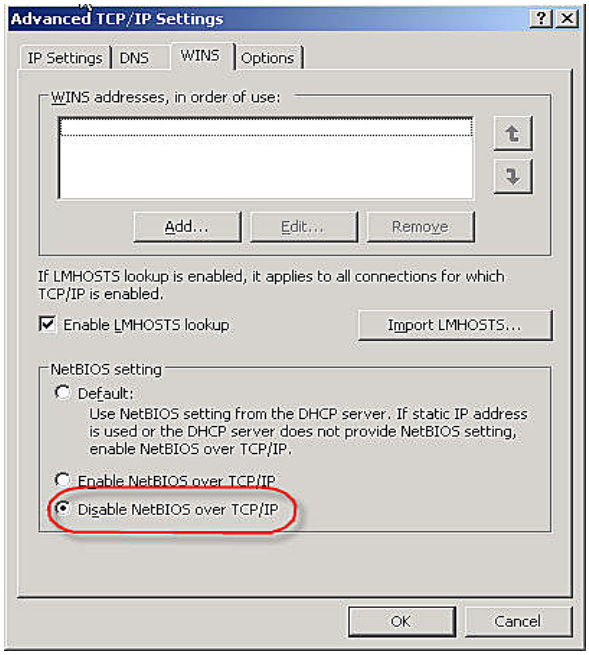
f After the Secondary server starts, open Network Connections, right-click the VMware Channel network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 10 . 10 . 11
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

g Configure the appropriate VMware Channel IP address and Subnet mask. Click **Advanced**.



h Click the **DNS** tab, clear the **Register this connection's addresses in DNS** check box, and click **OK**.


Advanced TCP/IP Settings
IP Settings
DNS
WINS
Options
WINS addresses, in order of use:
Add...
Edit...
Remove
If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.
Enable LMHOSTS lookup
Import LMHOSTS...
NetBIOS setting
Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
Enable NetBIOS over TCP/IP
Disable NetBIOS over TCP/IP
OK
Cancel

i Click the WINS tab, select **Disable NetBIOS over TCP/IP** and click **OK** twice.

j Select the Principal (Public) network connection, right-click and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Set the appropriate IP address (same as the Primary server for LAN installations), Subnet Mask, and Default Gateway, and click **OK**.

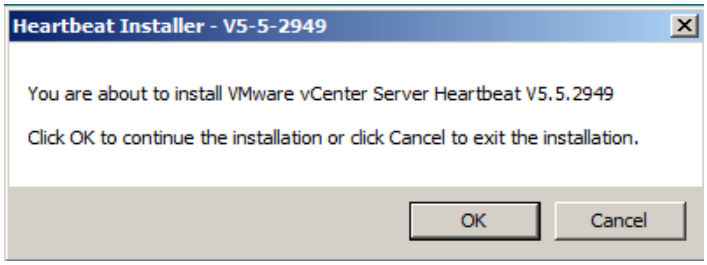
k In Network Connections, click **Advanced** and select **Advanced Settings**. Verify that the Principal (Public) NIC IP address is listed first in the Bind Order, and click **OK**.

l Right-click the Secondary (cloned) server image and select **Edit Settings**.

m Select the VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. IP communications with the Secondary server go through the VMware Channel.

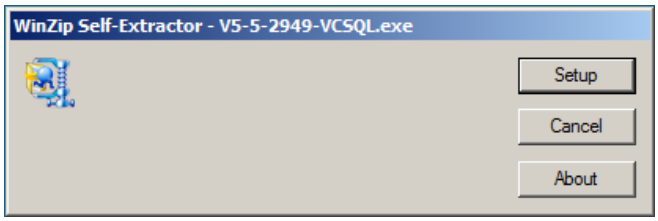
NOTE Do not connect the Principal (Public) virtual network adapter at this time to avoid an IP address conflict on the network.

2 Double-click the WinZip Self Extracting file to initiate the installation process. The **Setup Introduction** window is displayed. Review the information and click **OK**.

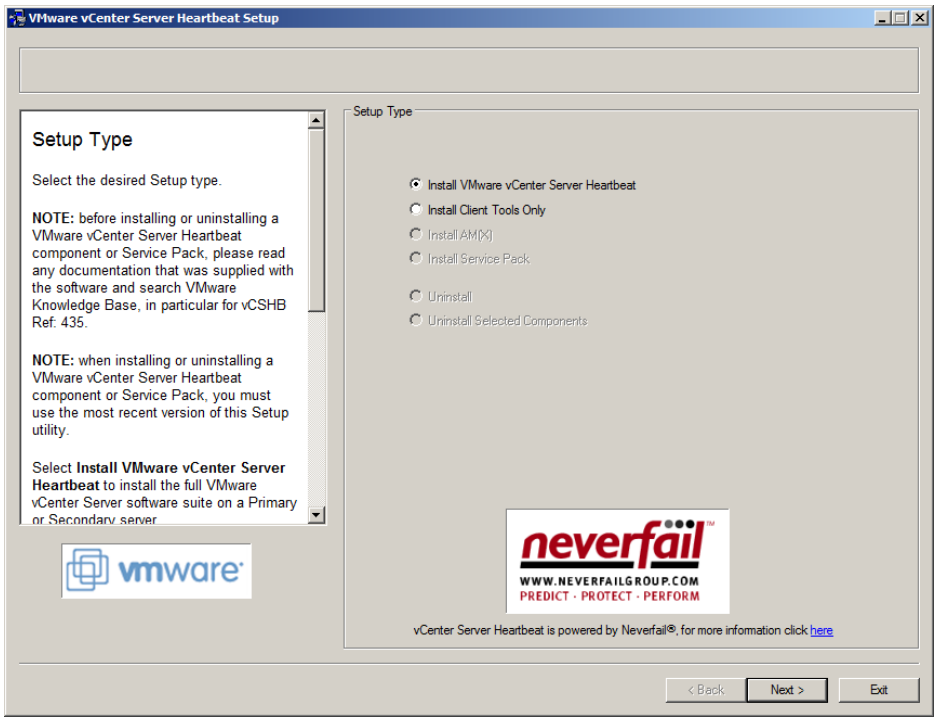

Heartbeat Installer - V5-5-2949
You are about to install VMware vCenter Server Heartbeat V5.5.2949
Click OK to continue the installation or click Cancel to exit the installation.
OK
Cancel

NOTE If you click Exit after Setup has started, you are prompted to save your settings. When you run the self extracting WinZip file again later, you will be asked if you want to use the previously saved configuration.

3 The **WinZip Self-Extractor** window is displayed. Click **Setup** to continue.

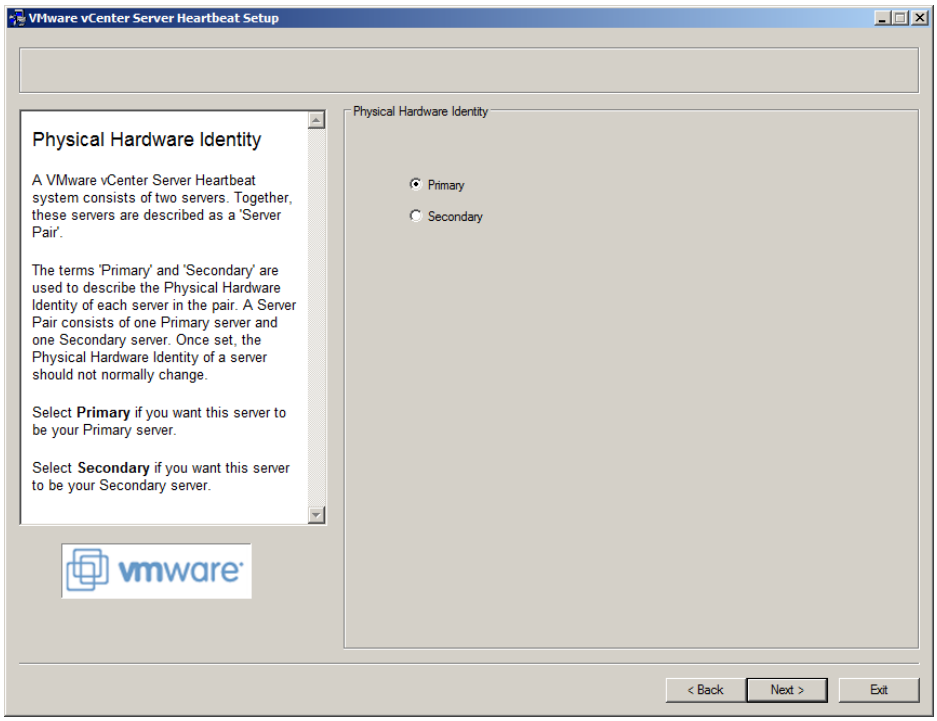


4 The **Setup Type** page is displayed. Because this is a new installation of vCenter Server Heartbeat, select **Install vCenter Server Heartbeat** and click **Next**.


VMware vCenter Server Heartbeat Setup
Setup Type
Select the desired Setup type.
NOTE: before installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, please read any documentation that was supplied with the software and search VMware Knowledge Base, in particular for vCSHB Ref: 435.
NOTE: when installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, you must use the most recent version of this Setup utility.
Select Install VMware vCenter Server Heartbeat to install the full VMware vCenter Server software suite on a Primary or Secondary server
Setup Type
Install VMware vCenter Server Heartbeat
Install Client Tools Only
Install AM(X)
Install Service Pack
Uninstall
Uninstall Selected Components
vmware
neverfail
WWW.NEVERFAILGROUP.COM
PREDICT · PROTECT · PERFORM
vCenter Server Heartbeat is powered by Neverfail®, for more information click here
< Back
Next >
Exit

NOTE The left pane of each page in the setup wizard provides information about the setup process.

5 Select the identity of the server through the **Physical Hardware Identity** page. Select **Primary** as the server identity and click **Next**.


VMware vCenter Server Heartbeat Setup
Physical Hardware Identity
A VMware vCenter Server Heartbeat system consists of two servers. Together, these servers are described as a 'Server Pair'.
The terms 'Primary' and 'Secondary' are used to describe the Physical Hardware Identity of each server in the pair. A Server Pair consists of one Primary server and one Secondary server. Once set, the Physical Hardware Identity of a server should not normally change.
Select Primary if you want this server to be your Primary server.
Select Secondary if you want this server to be your Secondary server.
vmware
Physical Hardware Identity
Primary
Secondary
< Back
Next >
Exit

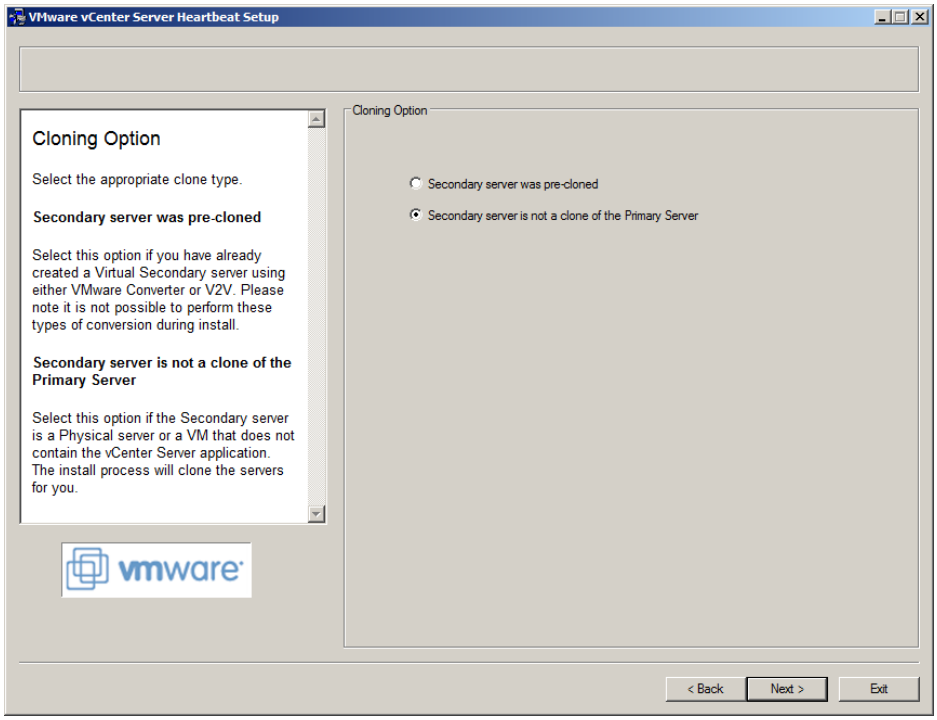
NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

Select the cloning options. If using the Install Clone technique, go to Step 6. If using the Pre-Clone technique, click the link below to jump to the Pre-Clone technique instructions.

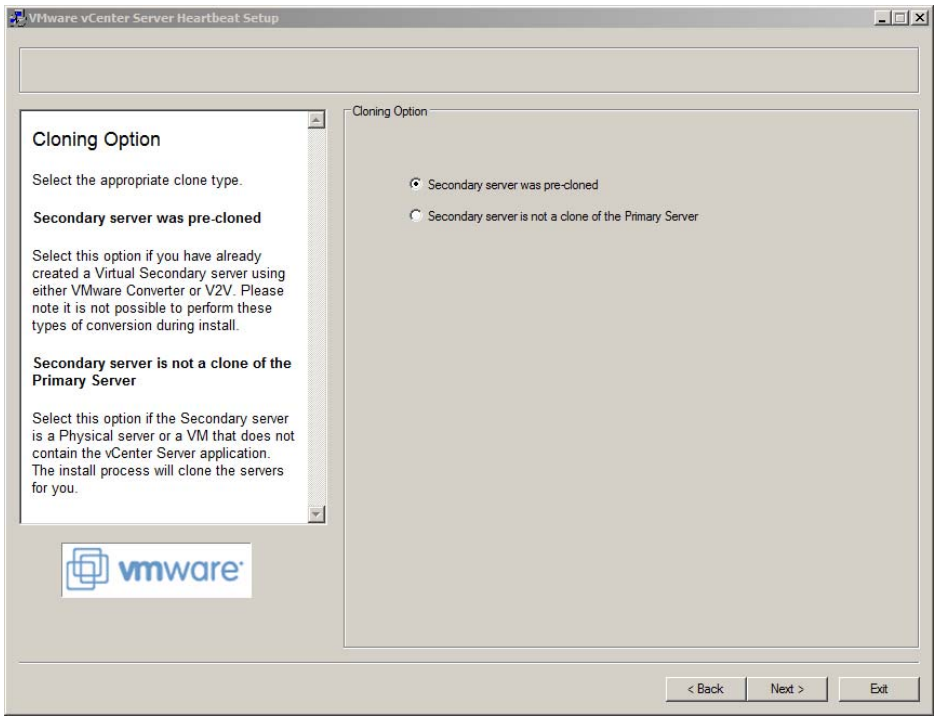
You have the following options:

- For installation using the Install Clone technique, continue with Step 6.
- For installation using the Pre-Clone technique, continue with Step 7.

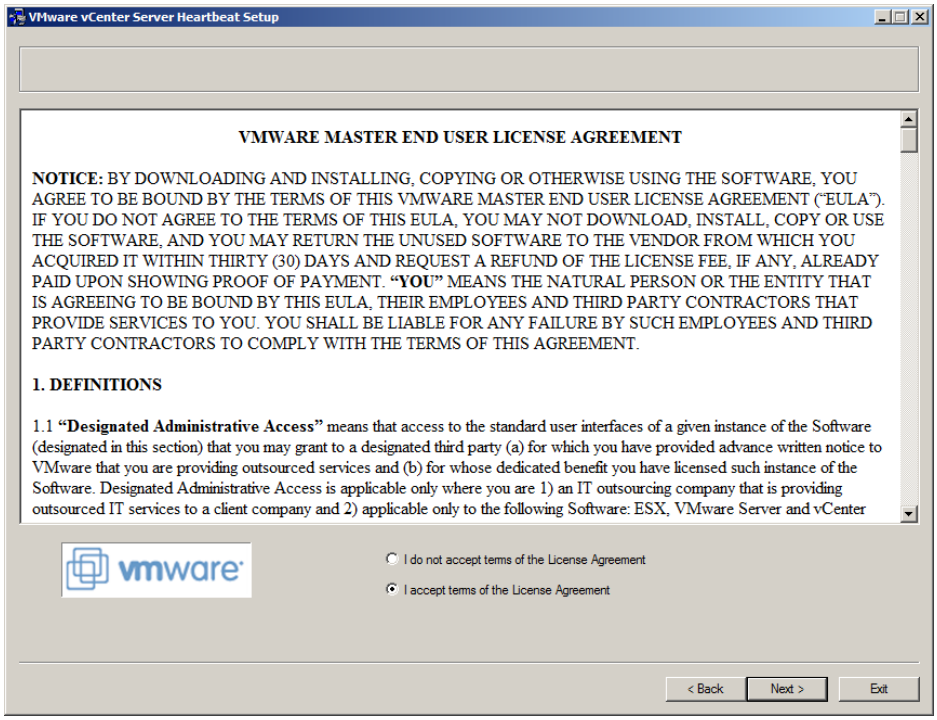
6 Select **Secondary server is not a clone of the Primary server** and click **Next** and go to Step 8.


VMware vCenter Server Heartbeat Setup
Cloning Option
Select the appropriate clone type.
Secondary server was pre-cloned
Select this option if you have already created a Virtual Secondary server using either VMware Converter or V2V. Please note it is not possible to perform these types of conversion during install.
Secondary server is not a clone of the Primary Server
Select this option if the Secondary server is a Physical server or a VM that does not contain the vCenter Server application. The install process will clone the servers for you.
Cloning Option
Secondary server was pre-cloned
Secondary server is not a clone of the Primary Server
vmware
< Back
Next >
Exit

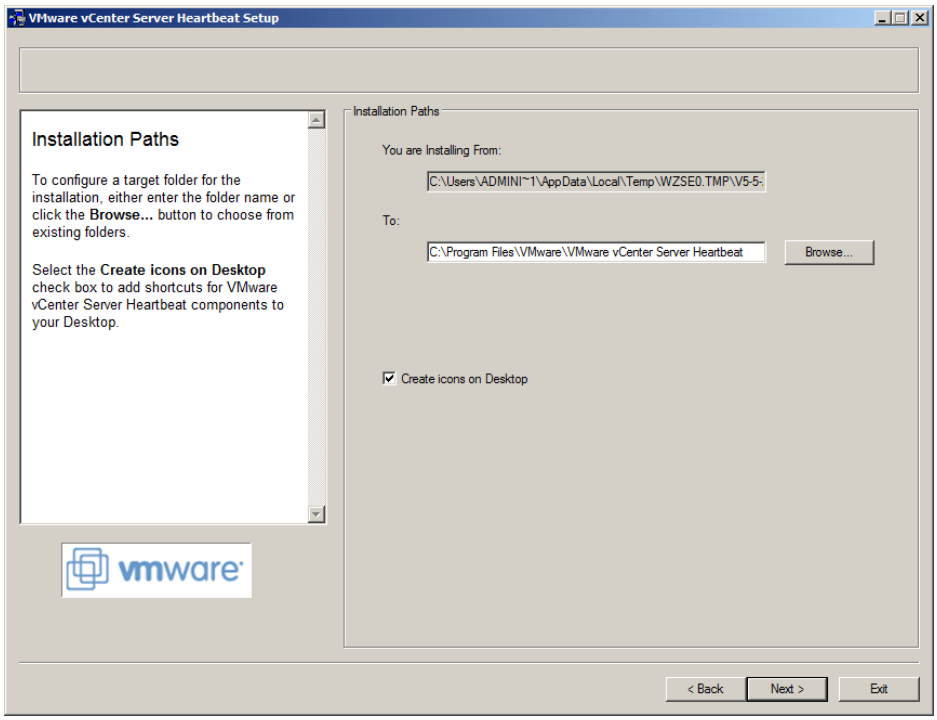
7 If a virtual Secondary server was created using the VMware Converter, the cloning option in the Virtual Infrastructure Client, or a third-party utility, select **Secondary server was pre-cloned** and click **Next**.


VMware vCenter Server Heartbeat Setup
Cloning Option
Select the appropriate clone type.
Secondary server was pre-cloned
Select this option if you have already created a Virtual Secondary server using either VMware Converter or V2V. Please note it is not possible to perform these types of conversion during install.
Secondary server is not a clone of the Primary Server
Select this option if the Secondary server is a Physical server or a VM that does not contain the vCenter Server application. The install process will clone the servers for you.
Cloning Option
Secondary server was pre-cloned
Secondary server is not a clone of the Primary Server
vmware
< Back
Next >
Exit

8 Read the license agreement carefully, select **I accept the terms of the License Agreement**, and click **Next**.


VMware vCenter Server Heartbeat Setup
VMWARE MASTER END USER LICENSE AGREEMENT
NOTICE: BY DOWNLOADING AND INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS VMWARE MASTER END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT DOWNLOAD, INSTALL, COPY OR USE THE SOFTWARE, AND YOU MAY RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, ALREADY PAID UPON SHOWING PROOF OF PAYMENT. "YOU" MEANS THE NATURAL PERSON OR THE ENTITY THAT IS AGREEING TO BE BOUND BY THIS EULA, THEIR EMPLOYEES AND THIRD PARTY CONTRACTORS THAT PROVIDE SERVICES TO YOU. YOU SHALL BE LIABLE FOR ANY FAILURE BY SUCH EMPLOYEES AND THIRD PARTY CONTRACTORS TO COMPLY WITH THE TERMS OF THIS AGREEMENT.
1. DEFINITIONS
1.1 "Designated Administrative Access" means that access to the standard user interfaces of a given instance of the Software (designated in this section) that you may grant to a designated third party (a) for which you have provided advance written notice to VMware that you are providing outsourced services and (b) for whose dedicated benefit you have licensed such instance of the Software. Designated Administrative Access is applicable only where you are 1) an IT outsourcing company that is providing outsourced IT services to a client company and 2) applicable only to the following Software: ESX, VMware Server and vCenter
vmware
I do not accept terms of the License Agreement
I accept terms of the License Agreement
< Back
Next >
Exit

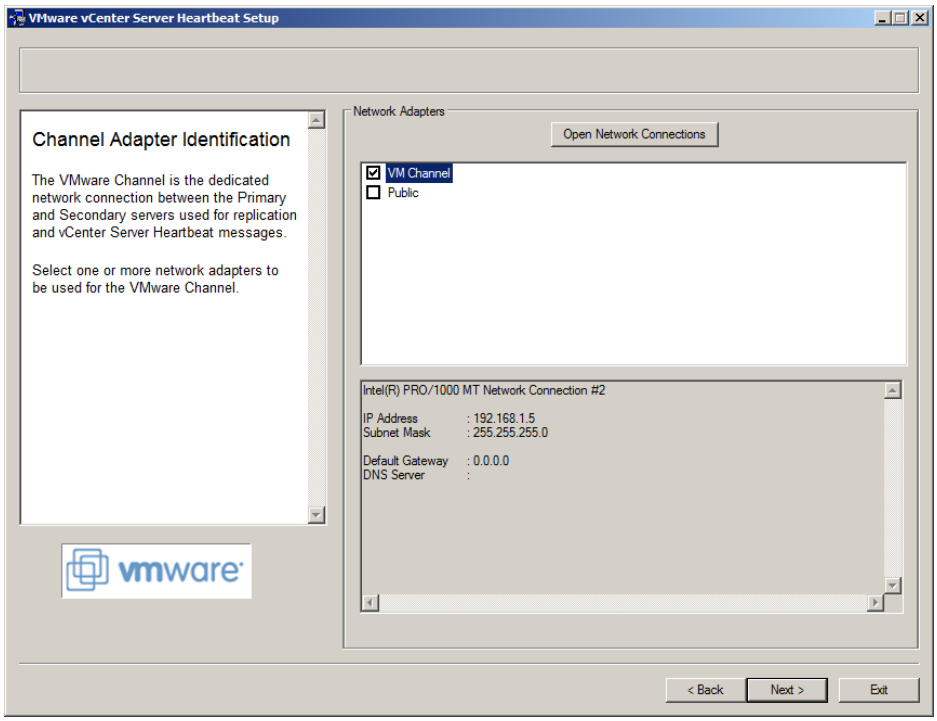
9 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.


VMware vCenter Server Heartbeat Setup
Installation Paths
To configure a target folder for the installation, either enter the folder name or click the Browse... button to choose from existing folders.
Select the Create icons on Desktop check box to add shortcuts for VMware vCenter Server Heartbeat components to your Desktop.
vmware
Installation Paths
You are Installing From:
C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-
To:
C:\Program Files\VMware\VMware vCenter Server Heartbeat
Browse...
Create icons on Desktop
< Back
Next >
Exit

NOTE The path of the VMware installation folder cannot contain Unicode characters. If vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, this causes the Neverfail Server R2 service to fail to start. The path of the VMware installation folder can only contain lower and upper case letters A to Z, digits from 0 to 9, and the following special characters: space \ _ - ( ) . :

Alternatively, click **Browse** to select one of these locations. Select Create icons on Desktop and click **Next**.

10 The **Channel Adapter Identification** page lets you identify the network adapter(s) for use in the VMware Channel. Select the network adapters (NICs) for the VMware Channel from the list. Click the adapter name to display the selected NIC properties in the lower panel. You must select at least one NIC to proceed with the installation. Click **Next**.


VMware vCenter Server Heartbeat Setup
Channel Adapter Identification
The VMware Channel is the dedicated network connection between the Primary and Secondary servers used for replication and vCenter Server Heartbeat messages.
Select one or more network adapters to be used for the VMware Channel.
vmware
Network Adapters
Open Network Connections
VM Channel
Public
Intel(R) PRO/1000 MT Network Connection #2
IP Address : 192.168.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
DNS Server :
< Back
Next >
Exit

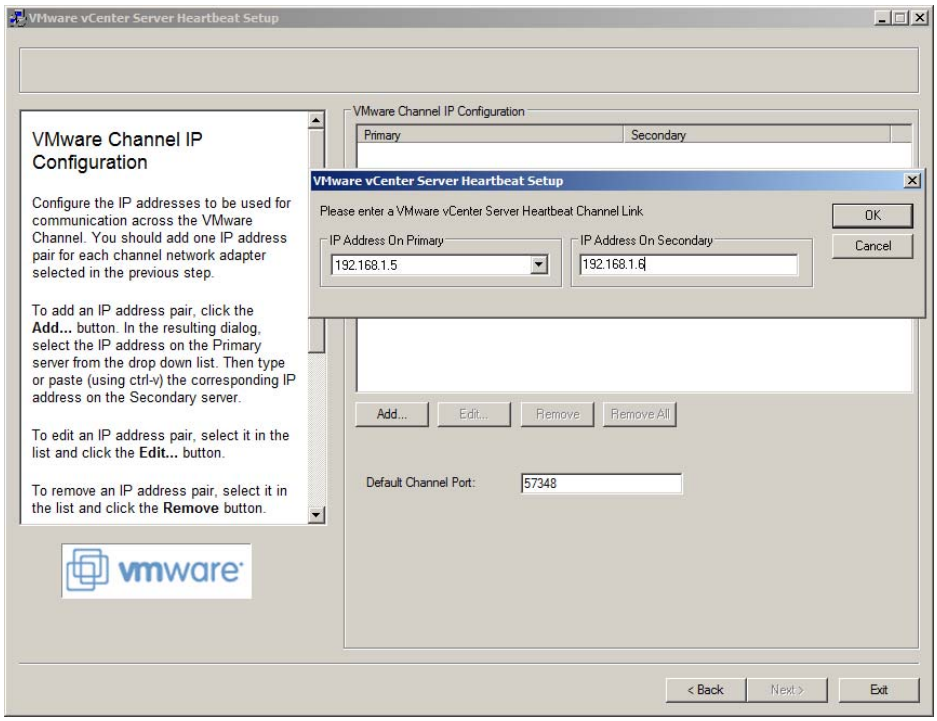
11 If no NICs are available, click **Open Network Connections** to review the network configuration of your machine and verify that you have the correct number of NICs installed.

NOTE Only one channel can be configured for each NIC. To configure more than one channel you must identify more than one NIC. A disabled NIC does not appear in this list. Enable the NIC to display it. If a NIC is disconnected, its IP addresses do not display in the lower panel.

---

12 The **VMware Channel IP Configuration** page prompts you to configure the VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. Type the VMware Channel IP addresses for both the Primary and Secondary servers. For the Primary server, select from a drop-down menu that lists all local IP addresses. Type the corresponding IP address on the Secondary server into the

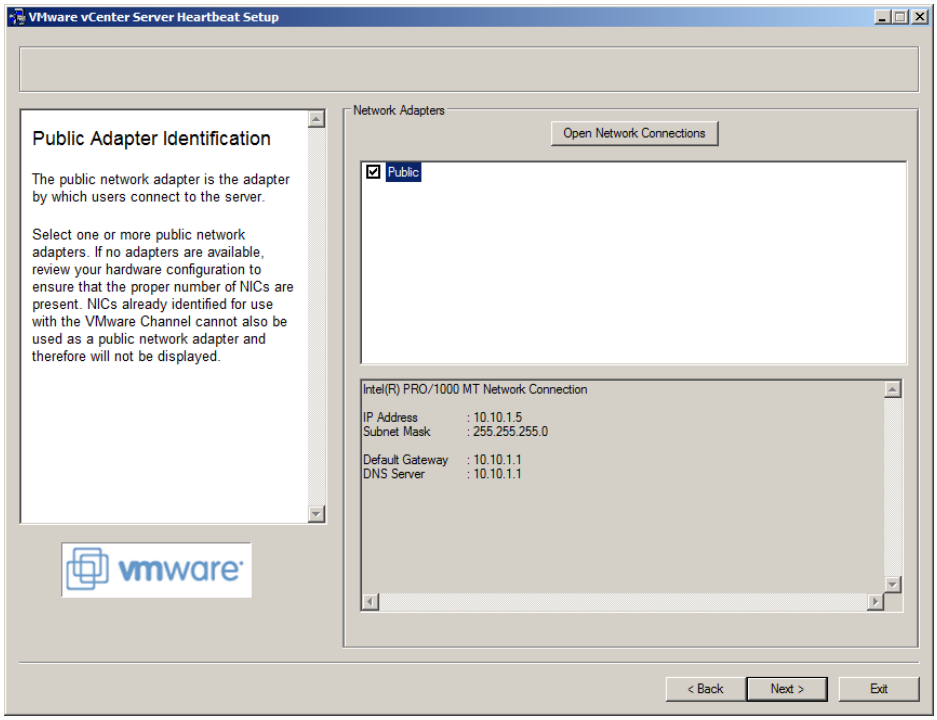
IP Address On Secondary text box. You must specify all VMware Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card. Click **OK**. Repeat this step for additional NICs.


VMware vCenter Server Heartbeat Setup
VMware Channel IP Configuration
Configure the IP addresses to be used for communication across the VMware Channel. You should add one IP address pair for each channel network adapter selected in the previous step.
To add an IP address pair, click the Add... button. In the resulting dialog, select the IP address on the Primary server from the drop down list. Then type or paste (using ctrl-v) the corresponding IP address on the Secondary server.
To edit an IP address pair, select it in the list and click the Edit... button.
To remove an IP address pair, select it in the list and click the Remove button.
vmware
VMware Channel IP Configuration
Primary
Secondary
VMware vCenter Server Heartbeat Setup
Please enter a VMware vCenter Server Heartbeat Channel Link
IP Address On Primary
192.168.1.5
IP Address On Secondary
192.168.1.6
OK
Cancel
Add...
Edit...
Remove
Remove All
Default Channel Port:
57348
< Back
Next >
Exit

13 Review and adjust, if necessary, the default channel port. Click **Next**.

NOTE When the implementation spans multiple sites with firewalls between the servers, configure the firewalls to allow traffic to pass through the default channel port or the manually configured channel port. Consult the VMware knowledge base for additional information.

14 Select the Principal (Public) NIC(s). The IP address information is displayed for each NIC.


VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
vmware
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
< Back
Next >
Exit

vCenter Server Heartbeat software can be deployed in a configuration where both servers have the same Principal (Public) IP address, for instance, in a standard Local Area Network (LAN) deployment where both machines are in the same subnet.

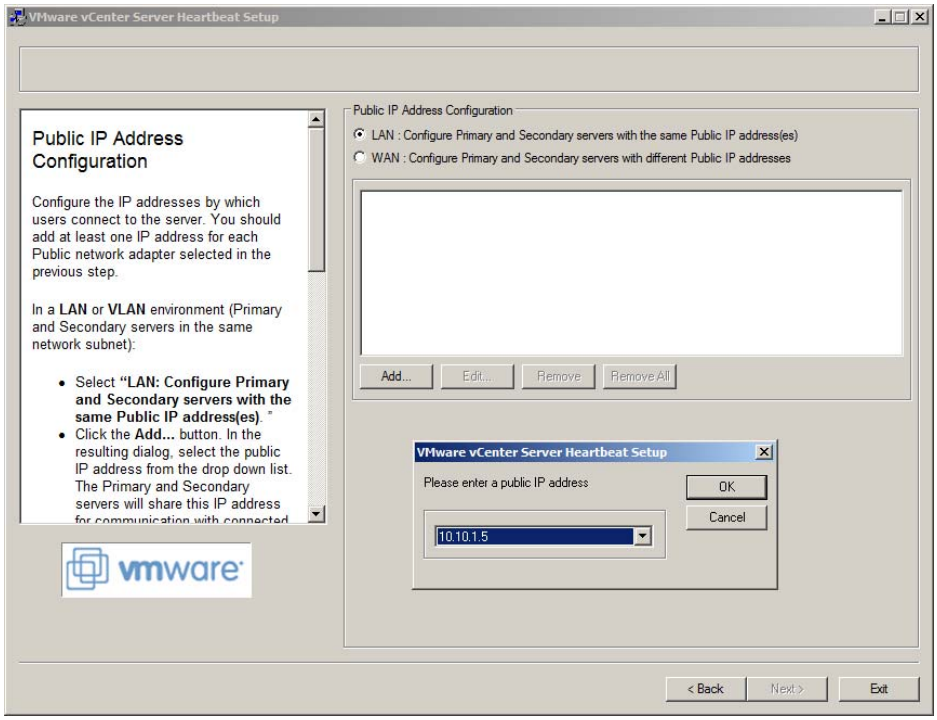
Alternatively vCenter Server Heartbeat can be deployed where the Principal (Public) IP addresses differ, for instance, in a Wide Area Network (WAN) deployment where the Primary and Secondary servers are located in different sites and subnets where client access is therefore bound by the standard network routing to allow the correct connectivity to the server according to its locale.

15 Select **LAN: Configure Primary and Secondary servers with the same Public IP addresses** or **WAN: Configure Primary and Secondary servers with different Public IP addresses**.

You have the following options:

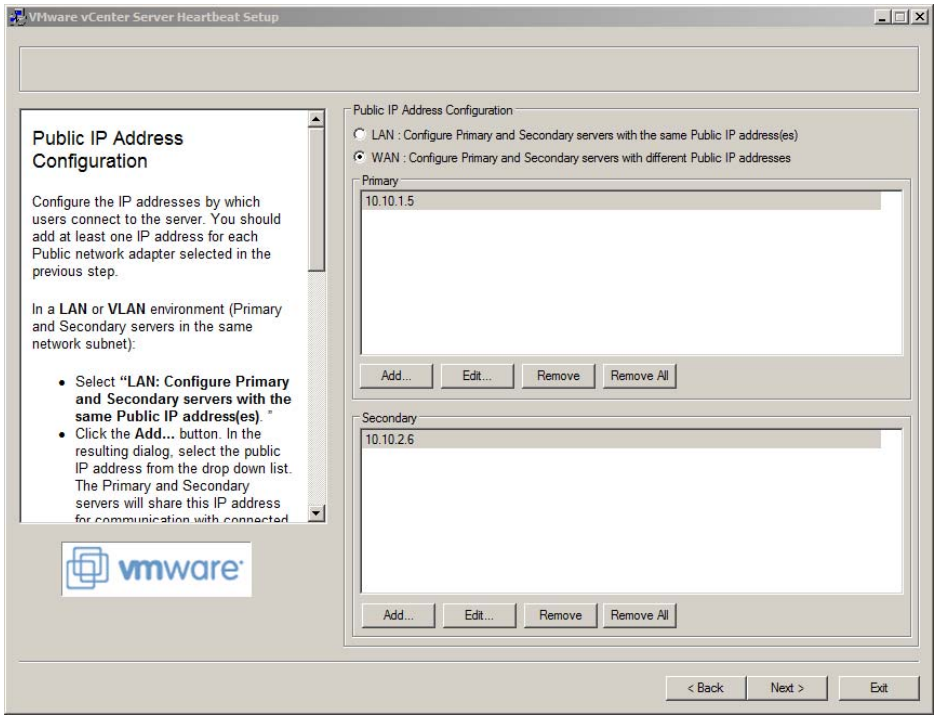
- For a WAN installation with different subnets, go to Step 17.
- For LAN installation or same subnet WAN installs, continue with Step 16.

16 For a LAN environment, click **Add** to specify the IP address.


VMware vCenter Server Heartbeat Setup
Public IP Address Configuration
Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Public network adapter selected in the previous step.
In a LAN or VLAN environment (Primary and Secondary servers in the same network subnet):
Select "LAN: Configure Primary and Secondary servers with the same Public IP address(es)."
Click the Add... button. In the resulting dialog, select the public IP address from the drop down list. The Primary and Secondary servers will share this IP address
Public IP Address Configuration
LAN : Configure Primary and Secondary servers with the same Public IP address(es)
WAN : Configure Primary and Secondary servers with different Public IP addresses
Add...
Edit...
Remove
Remove All
VMware vCenter Server Heartbeat Setup
Please enter a public IP address
OK
Cancel
10.10.1.5
vmware
< Back
Next >
Exit

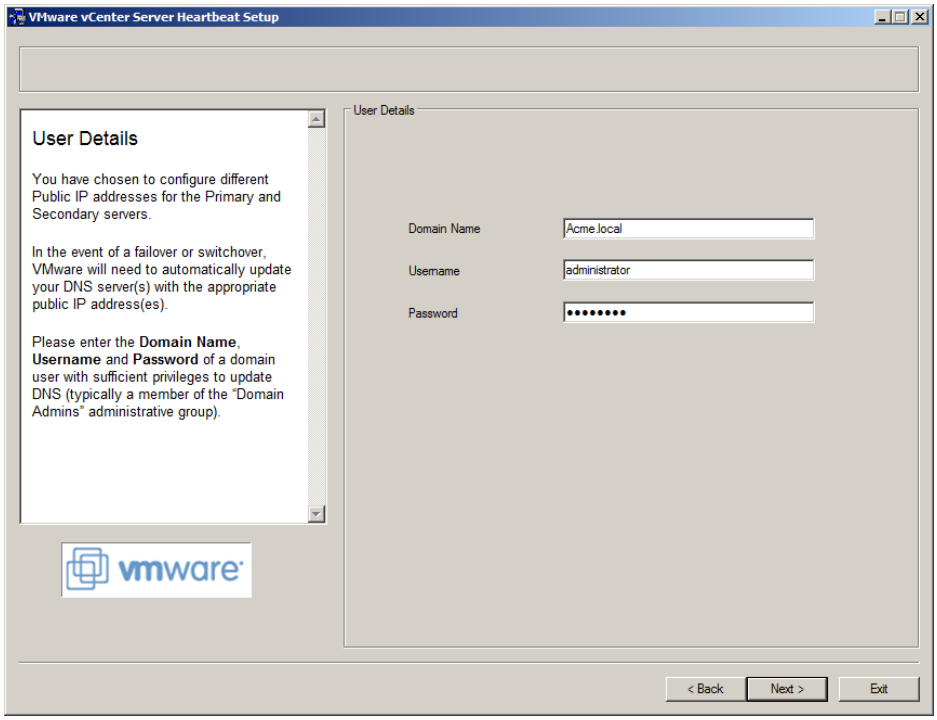
If installing in a LAN or when the WAN uses the same subnet, go to Step 20.

17 For a WAN environment, specify IP addresses for both Primary and Secondary servers.


VMware vCenter Server Heartbeat Setup
Public IP Address Configuration
Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Public network adapter selected in the previous step.
In a LAN or VLAN environment (Primary and Secondary servers in the same network subnet):
Select "LAN: Configure Primary and Secondary servers with the same Public IP address(es)."
Click the Add... button. In the resulting dialog, select the public IP address from the drop down list. The Primary and Secondary servers will share this IP address
Public IP Address Configuration
LAN : Configure Primary and Secondary servers with the same Public IP address(es)
WAN : Configure Primary and Secondary servers with different Public IP addresses
Primary
10.10.1.5
Add...
Edit...
Remove
Remove All
Secondary
10.10.2.6
Add...
Edit...
Remove
Remove All
vmware
< Back
Next >
Exit

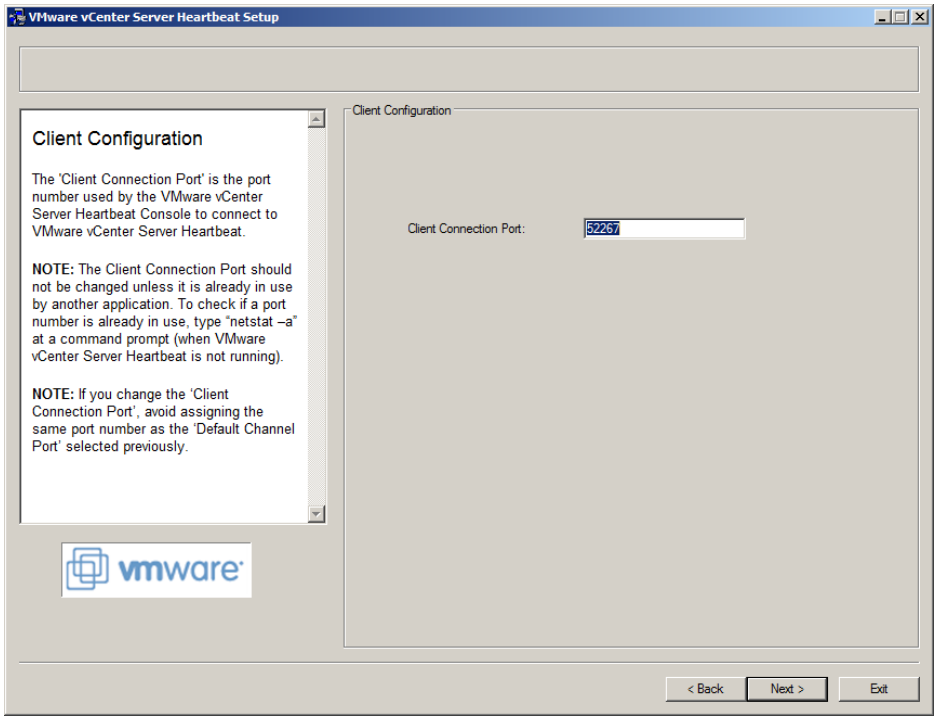
18 Add each Principal (Public) network address until all addresses are present. Click **Next**.

19 When the Principal (Public) addresses on the Secondary server are different from those on the Primary server, vCenter Server Heartbeat must perform additional tasks during failover or switchover. These additional tasks require clients to change their resolution of the active server to a different IP address and requires that vCenter Server Heartbeat update the DNS entries for the active server across the enterprise. Such updates require credentials for domain administrators (or an account with equivalent rights). Type the **Domain Name**, a domain administrator **Username** and **Password** into the respective text boxes and click **Next**.


VMware vCenter Server Heartbeat Setup
User Details
You have chosen to configure different Public IP addresses for the Primary and Secondary servers.
In the event of a failover or switchover, VMware will need to automatically update your DNS server(s) with the appropriate public IP address(es).
Please enter the Domain Name, Username and Password of a domain user with sufficient privileges to update DNS (typically a member of the "Domain Admins" administrative group).
vmware
User Details
Domain Name
Acme.local
Username
administrator
Password
< Back
Next >
Exit

The vCenter Server Heartbeat server pair can be administered remotely on client machines using the vCenter Server Heartbeat Console.

20 The vCenter Server Heartbeat Console connects to an IP address of the active server using the default client connection port of 52267. If this port is already in use, type an available client connection port. Click **Next**.


VMware vCenter Server Heartbeat Setup
Client Configuration
The 'Client Connection Port' is the port number used by the VMware vCenter Server Heartbeat Console to connect to VMware vCenter Server Heartbeat.
NOTE: The Client Connection Port should not be changed unless it is already in use by another application. To check if a port number is already in use, type "netstat –a" at a command prompt (when VMware vCenter Server Heartbeat is not running).
NOTE: If you change the 'Client Connection Port', avoid assigning the same port number as the 'Default Channel Port' selected previously.
vmware
Client Configuration
Client Connection Port:
52267
< Back
Next >
Exit

21 Select the applications to protect. All licensed vCenter Server Heartbeat features are listed.

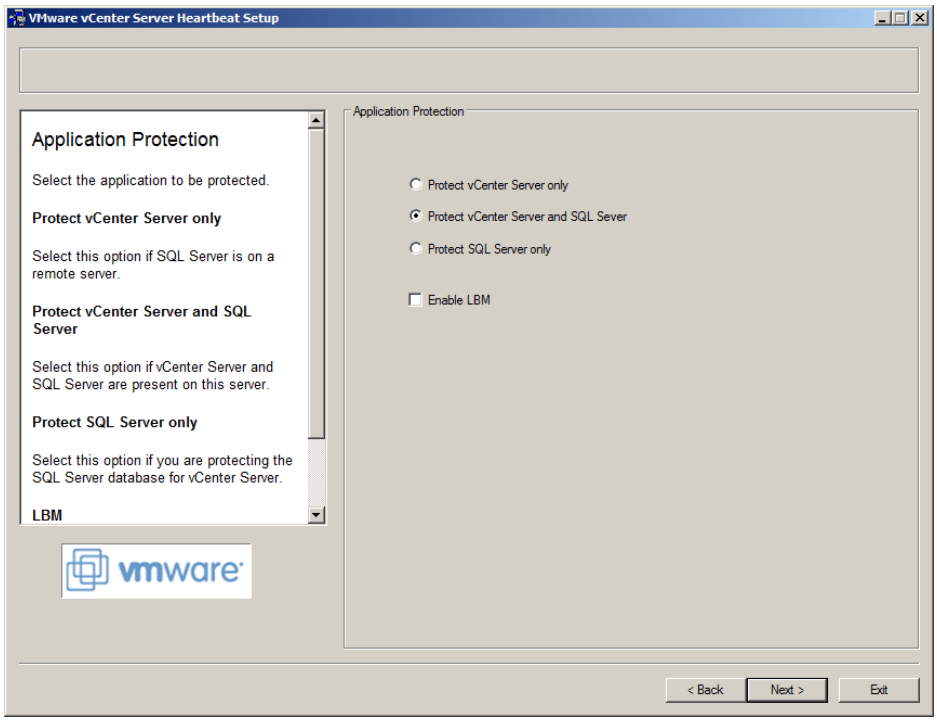
If installing vCenter Server only, or vCenter Server locally and the SQL Server on a separate server, select **Protect Virtual Center only**.

If installing SQL Server remotely, upon completion of the vCenter Server installation locally, repeat the installation procedure at the remote SQL Server location and select **Protect SQL Server only**.

If installing both vCenter Server and SQL Server locally, select **Protect Virtual Center and SQL Server**.

Select the applications to protect. If installing in a WAN, enable the Low Bandwidth Module by selecting **Enable LBM**. Click **Next**.

CAUTION Do not enable the Low Bandwidth Module (LBM) for a LAN install.


VMware vCenter Server Heartbeat Setup
Application Protection
Select the application to be protected.
Protect vCenter Server only
Select this option if SQL Server is on a remote server.
Protect vCenter Server and SQL Server
Select this option if vCenter Server and SQL Server are present on this server.
Protect SQL Server only
Select this option if you are protecting the SQL Server database for vCenter Server.
LBM
vmware
Application Protection
Protect vCenter Server only
Protect vCenter Server and SQL Sever
Protect SQL Server only
Enable LBM
< Back
Next >
Exit

22 To facilitate the clone of the Primary server onto the Secondary server, you must back up pertinent components of the Primary server for restoration on to the Secondary server. Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server.

Where the VMware Channel connection is slower than 10 Mbit/s or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

You have the following options:

- For installation using the Pre-Clone technique, go to Step a of Step 23 on page 87.
- For installation using the Install Clone technique, continue with Step a of Step 22.

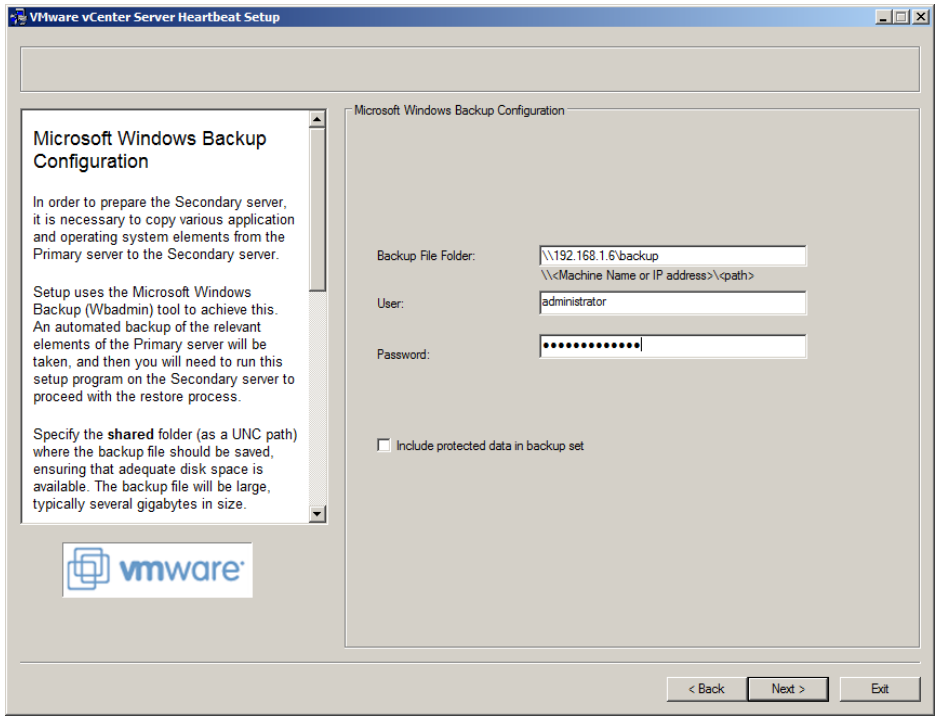
Continue with Step a.

a Configure Microsoft Windows Backup options. Depending on the network topology between the servers, backup files can include or exclude application data. Including application data in the backup file decreases the time to initially verify and synchronize the applications data on first start up of vCenter Server Heartbeat. This is useful where VMware Channel connections are slower than LAN speed, such as in a WAN implementation.

With Windows Server 2008, vCenter Server Heartbeat does not stop services and prevents downtime by using the Windows Volume Shadow Service to take the backup. Including the applications' protected data vastly increases the backup file size and therefore increases the time of the backup operation. Due to the potential large size of the backup file, careful consideration is required when including application data and specifying the backup folder location.

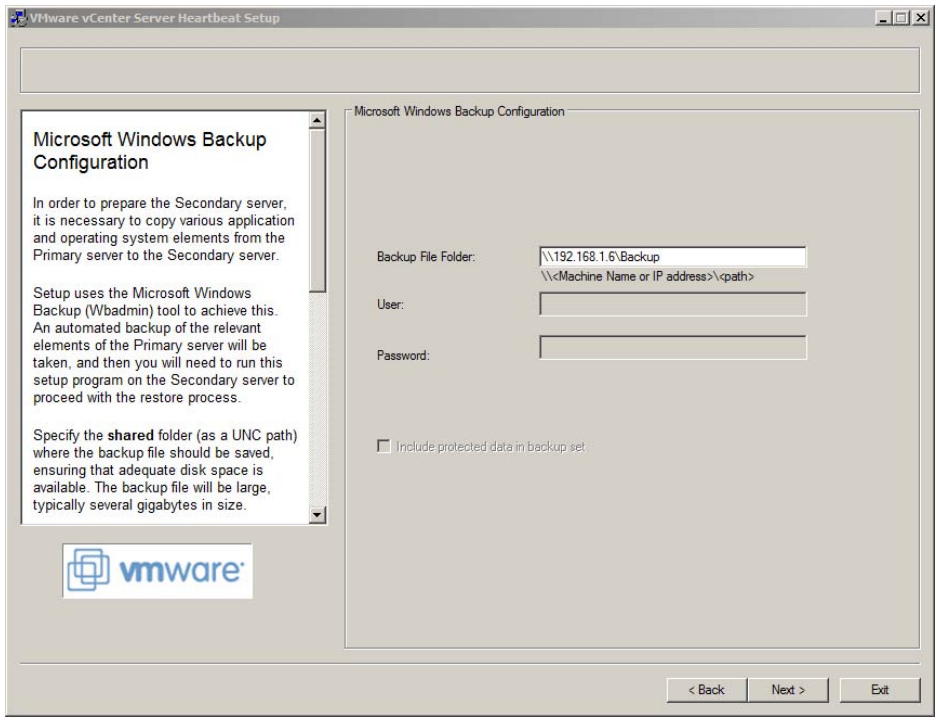
To estimate the maximum size of the backup file, add together the size of each volume that contains system data and application data. Although the actual size of the backup file can be smaller, using this rule of thumb helps ensure a successful installation.

Select a location to place the backup files through the **Microsoft Windows Backup Configuration** page. When installing into a Windows Server 2008 environment, you must specify a UNC path to the backup file location. Type a UNC path to a location using the machine name or IP address and shared folder into the **Folder** text box. Type a **User** and **Password** that grants access to the shared folder. Click **Next**.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Configuration
In order to prepare the Secondary server, it is necessary to copy various application and operating system elements from the Primary server to the Secondary server.
Setup uses the Microsoft Windows Backup (Wbadmin) tool to achieve this. An automated backup of the relevant elements of the Primary server will be taken, and then you will need to run this setup program on the Secondary server to proceed with the restore process.
Specify the shared folder (as a UNC path) where the backup file should be saved, ensuring that adequate disk space is available. The backup file will be large, typically several gigabytes in size.
vmware
Microsoft Windows Backup Configuration
Backup File Folder:
\\192.168.1.6\backup
\\<Machine Name or IP address>\<path>
User:
administrator
Password:
Include protected data in backup set
< Back
Next >
Exit

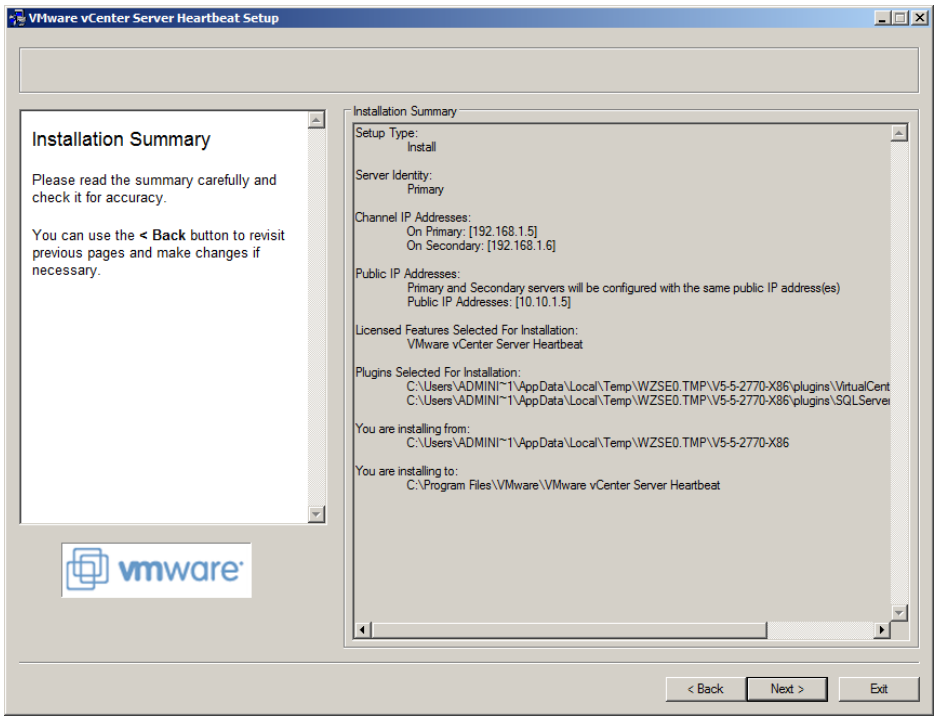
23 When selecting the Pre-Clone technique, Setup backs up two small files, nfsetup.dat and primary.csv, from the Primary server and restores them to the Secondary server for proper configuration.

a Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server. Type the machine name or IP address and the path to the shared folder to receive the backup files, for example: `\\192.168.1.6\Backup`.

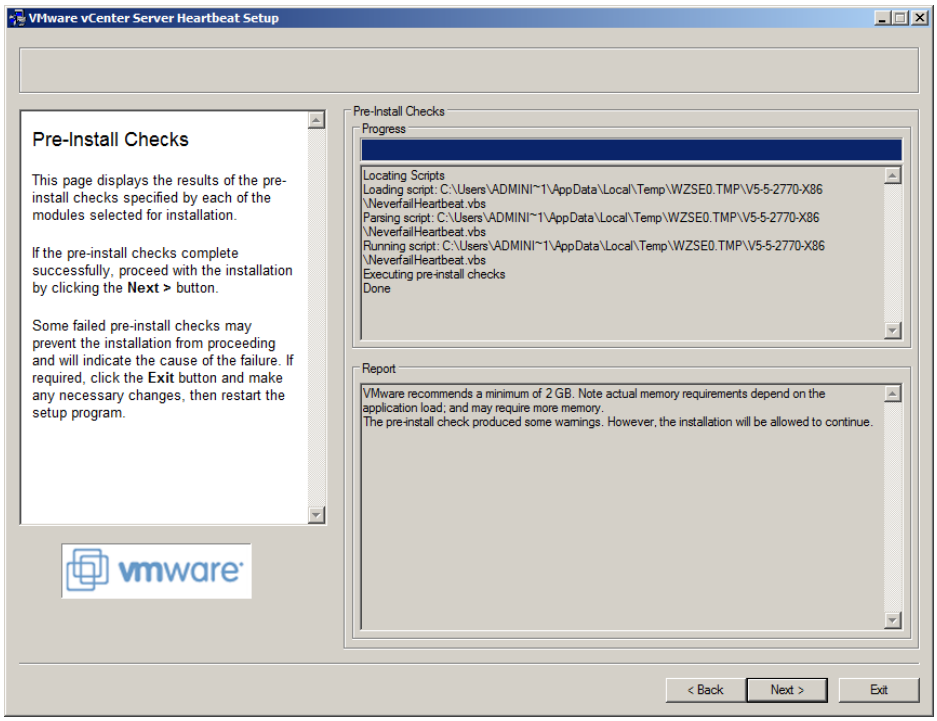

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Configuration
In order to prepare the Secondary server, it is necessary to copy various application and operating system elements from the Primary server to the Secondary server.
Setup uses the Microsoft Windows Backup (Wbadmin) tool to achieve this. An automated backup of the relevant elements of the Primary server will be taken, and then you will need to run this setup program on the Secondary server to proceed with the restore process.
Specify the shared folder (as a UNC path) where the backup file should be saved, ensuring that adequate disk space is available. The backup file will be large, typically several gigabytes in size.
Microsoft Windows Backup Configuration
Backup File Folder:
\\192.168.1.6\Backup
\\<Machine Name or IP address>\<path>
User:
Password:
Include protected data in backup set
vmware
< Back
Next >
Exit

b Where the VMware Channel connection is slower than 10 Mbit/s or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

24 Review the summary of options and configuration information for the installation. Click **Next**.



25 Pre-install checks run to ensure that the installation can continue. Setup checks the available disk space, system memory, operating system compatibility, and dependencies between modules. The Report panel displays the results of the pre-install checks.

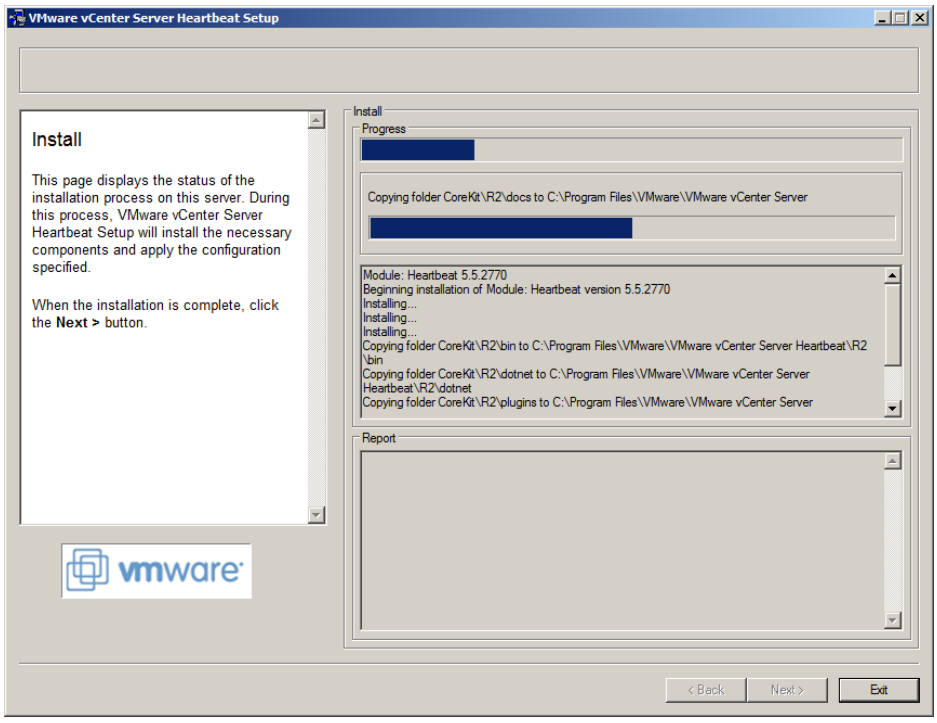

VMware vCenter Server Heartbeat Setup
Pre-Install Checks
This page displays the results of the pre-install checks specified by each of the modules selected for installation.
If the pre-install checks complete successfully, proceed with the installation by clicking the Next > button.
Some failed pre-install checks may prevent the installation from proceeding and will indicate the cause of the failure. If required, click the Exit button and make any necessary changes, then restart the setup program.
vmware
Pre-Install Checks
Progress
Locating Scripts
Loading script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Parsing script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Running script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE0.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Executing pre-install checks
Done
Report
VMware recommends a minimum of 2 GB. Note actual memory requirements depend on the application load; and may require more memory.
The pre-install check produced some warnings. However, the installation will be allowed to continue.
< Back
Next >
Exit

26 If some pre-install checks are unsuccessful, go back through the wizard and make the necessary changes, and run the pre-install checks again. If the pre-install checks are successful, click **Next**.

NOTE The **Progress** panel on the **Pre-Install Checks** page displays the progress of these checks. When finished, the Report panel displays the results.

27 The next page displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and configures it with the default settings.

NOTE If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version. To learn more about Heartbeat Diagnostics, see *Getting Started with Heartbeat Diagnostics* on the VMware Web site.


VMware vCenter Server Heartbeat Setup
Install
This page displays the status of the installation process on this server. During this process, VMware vCenter Server Heartbeat Setup will install the necessary components and apply the configuration specified.
When the installation is complete, click the Next > button.
vmware
Install
Progress
Copying folder CoreKit\R2\docs to C:\Program Files\VMware\VMware vCenter Server
Module: Heartbeat 5.5.2770
Beginning installation of Module: Heartbeat version 5.5.2770
Installing...
Installing...
Installing...
Copying folder CoreKit\R2\bin to C:\Program Files\VMware\VMware vCenter Server Heartbeat\R2\bin
Copying folder CoreKit\R2\dotnet to C:\Program Files\VMware\VMware vCenter Server Heartbeat\R2\dotnet
Copying folder CoreKit\R2\plugins to C:\Program Files\VMware\VMware vCenter Server
Report
< Back
Next >
Exit

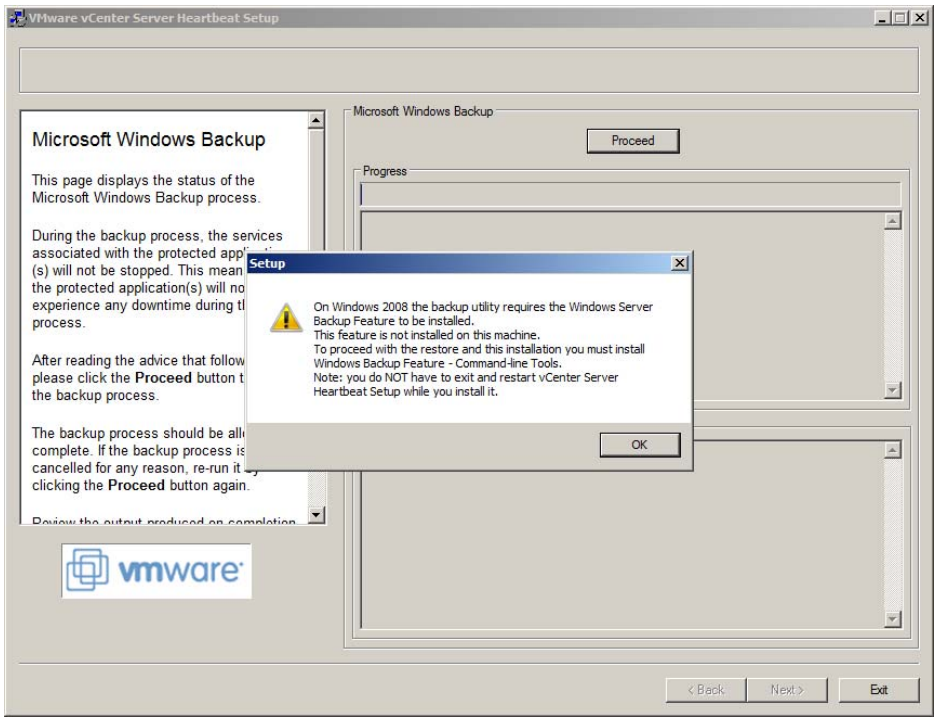
28 Click **Next** after vCenter Server Heartbeat components are complete.

You have the following options:

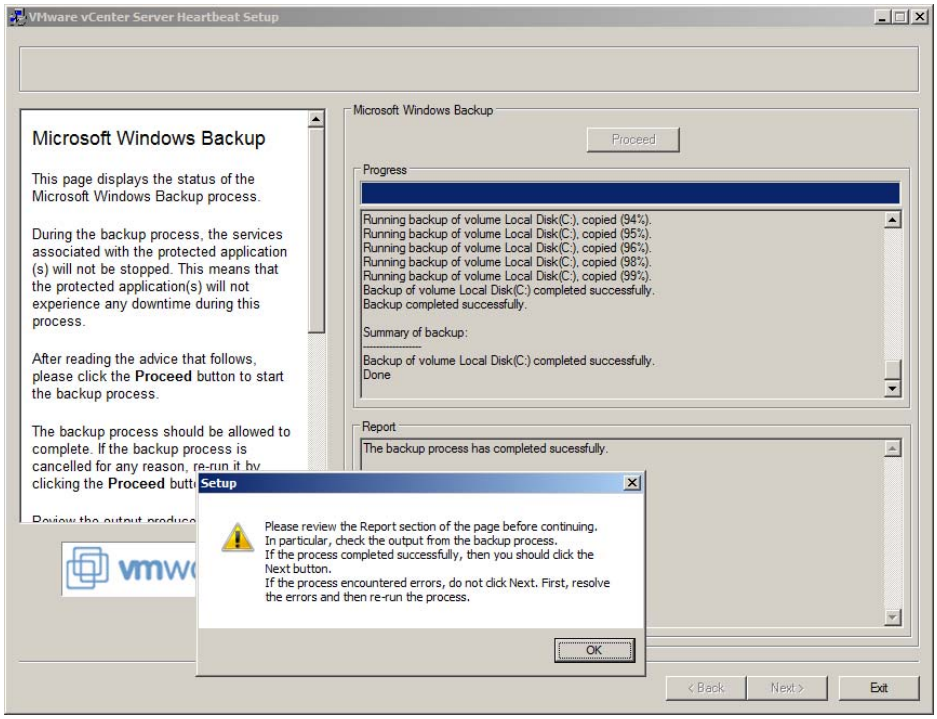
- If using the Pre-Clone installation technique, go to Step 31.
- If using the Install Clone installation technique, continue to Step 29.

29 The next page displays the status of the Microsoft Windows Backup process. The automated backup is saved in the previously defined location.

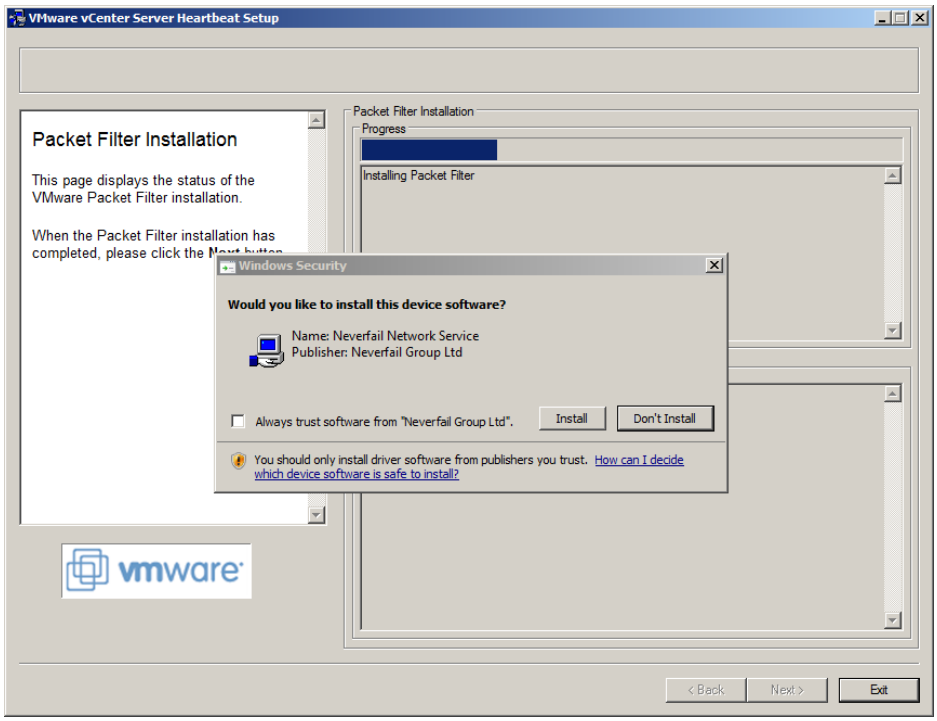
NOTE When installing into a Windows Server 2008 environment, vCenter Server Heartbeat verifies that the Windows Server Backup Feature and Command Line Tools are installed. If they are not installed, you must install them now. You are not required to exit the installation to install the Windows Server Backup Feature. Navigate to the Server Manager and under Features, add the Windows Backup Feature and Command Line Tools. When installing Windows Server Backup Feature, Windows PowerShell is also necessary.


VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup
This page displays the status of the Microsoft Windows Backup process.
During the backup process, the services associated with the protected appl
(s) will not be stopped. This mean
the protected application(s) will no
experience any downtime during th
process.
After reading the advice that follow
please click the Proceed button t
the backup process.
The backup process should be all
complete. If the backup process is
cancelled for any reason, re-run it
clicking the Proceed button again.
Microsoft Windows Backup
Proceed
Progress
Setup
On Windows 2008 the backup utility requires the Windows Server Backup Feature to be installed.
This feature is not installed on this machine.
To proceed with the restore and this installation you must install Windows Backup Feature - Command-line Tools.
Note: you do NOT have to exit and restart vCenter Server Heartbeat Setup while you install it.
OK
vmware
< Back
Next >
Exit

30 If required, install Windows Backup Feature – Command Line Tools. Click **Proceed**. The automated backup is saved in the previously defined location and the progress of the backup operation is displayed in the Progress panel. When finished, a report on the backup is displayed in the Report panel. Review the backup report to verify successful completion. Click **OK** on the window and click **Next** on the page.

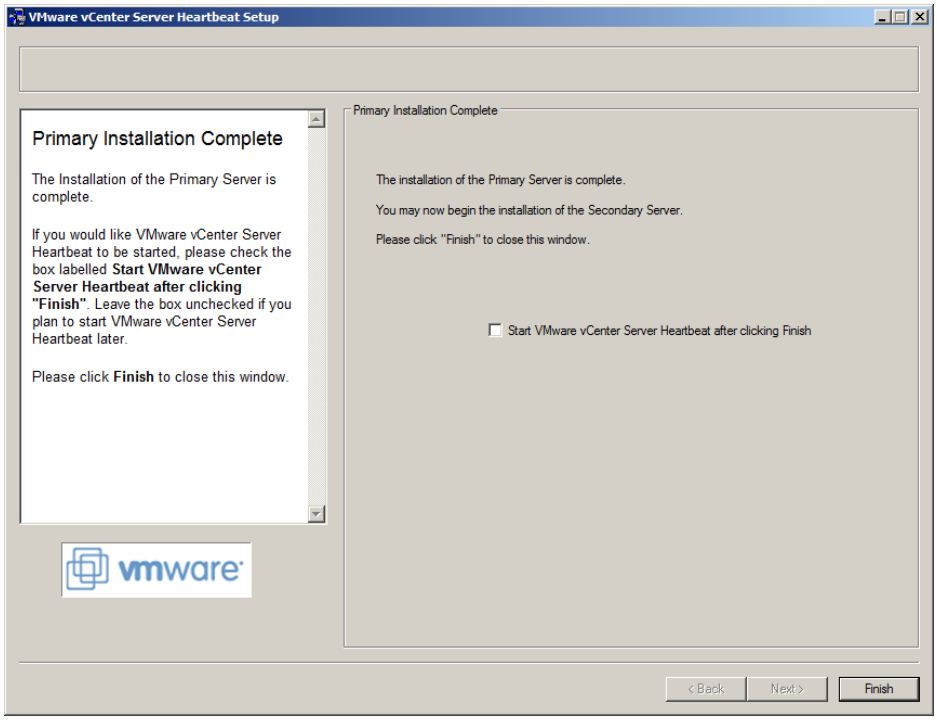

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup
This page displays the status of the Microsoft Windows Backup process.
During the backup process, the services associated with the protected application (s) will not be stopped. This means that the protected application(s) will not experience any downtime during this process.
After reading the advice that follows, please click the Proceed button to start the backup process.
The backup process should be allowed to complete. If the backup process is cancelled for any reason, re-run it by clicking the Proceed butt
Microsoft Windows Backup
Proceed
Progress
Running backup of volume Local Disk(C:), copied (94%).
Running backup of volume Local Disk(C:), copied (95%).
Running backup of volume Local Disk(C:), copied (96%).
Running backup of volume Local Disk(C:), copied (98%).
Running backup of volume Local Disk(C:), copied (99%).
Backup of volume Local Disk(C:) completed successfully.
Backup completed successfully.
Summary of backup:
Backup of volume Local Disk(C:) completed successfully.
Done
Report
The backup process has completed sucessfully.
Setup
Please review the Report section of the page before continuing.
In particular, check the output from the backup process.
If the process completed successfully, then you should click the Next button.
If the process encountered errors, do not click Next. First, resolve the errors and then re-run the process.
OK
< Back
Next >
Exit

31 The vCenter Server Heartbeat Packet Filter driver installs on each network card of the production server. If you see warnings that the driver is unsigned or did not complete the Windows Logo tests, click **Install**. If Windows is configured to display Signed Driver warnings, multiple warnings can appear. The lower panel displays the results of the process. Click **Next**.


VMware vCenter Server Heartbeat Setup
Packet Filter Installation
This page displays the status of the VMware Packet Filter installation.
When the Packet Filter installation has completed, please click the
Packet Filter Installation
Progress
Installing Packet Filter
Windows Security
Would you like to install this device software?
Name: Neverfail Network Service
Publisher: Neverfail Group Ltd
Always trust software from "Neverfail Group Ltd".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?
vmware
< Back
Next >
Exit

By default, the vCenter Server Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The vCenter Server Heartbeat Packet Filter is not applied to the network cards forming VMware Channel connections as these cards maintain unique IP addresses irrespective of the role of the server. vCenter Server Heartbeat also disables NetBIOS on the Channel NIC(s) to prevent domain name conflicts on the subnet.

32 When the setup wizard confirms the successful completion of the installation, click **Finish**.

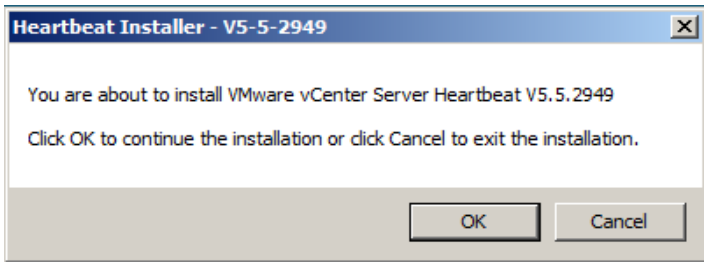

VMware vCenter Server Heartbeat Setup
Primary Installation Complete
The Installation of the Primary Server is complete.
If you would like VMware vCenter Server Heartbeat to be started, please check the box labelled Start VMware vCenter Server Heartbeat after clicking "Finish". Leave the box unchecked if you plan to start VMware vCenter Server Heartbeat later.
Please click Finish to close this window.
vmware
Primary Installation Complete
The installation of the Primary Server is complete.
You may now begin the installation of the Secondary Server.
Please click "Finish" to close this window.
Start VMware vCenter Server Heartbeat after clicking Finish
< Back
Next >
Finish

Secondary Server

The process of installing vCenter Server Heartbeat on the Secondary server is similar to installing vCenter Server Heartbeat on the Primary server.

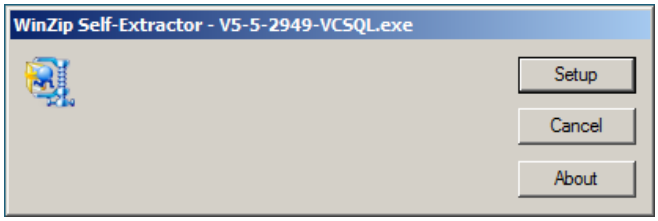
To install the Secondary server

1 To install the vCenter Server Heartbeat on the Secondary server, download the vCenter Server Heartbeat installer to a suitable location on the Secondary server. Execute the WinZip Self Extracting file to start the installation process. The **Setup Introduction** window is displayed. Review the information and click **OK**.

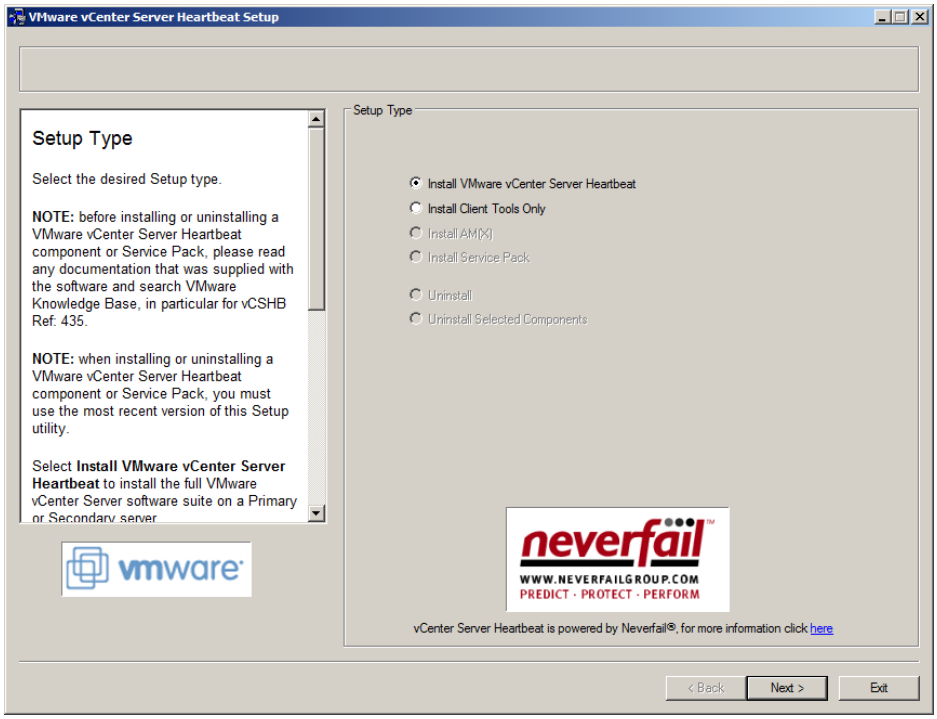

Heartbeat Installer - V5-5-2949
You are about to install VMware vCenter Server Heartbeat V5.5.2949
Click OK to continue the installation or click Cancel to exit the installation.
OK
Cancel

NOTE If you click **Exit** after Setup has started, you are prompted to save your settings. When you run the self extracting WinZip file again later, you will be asked if you want to use the previously saved configuration.

2 The **WinZip Self-Extractor** window is displayed. Click **Setup** to continue.

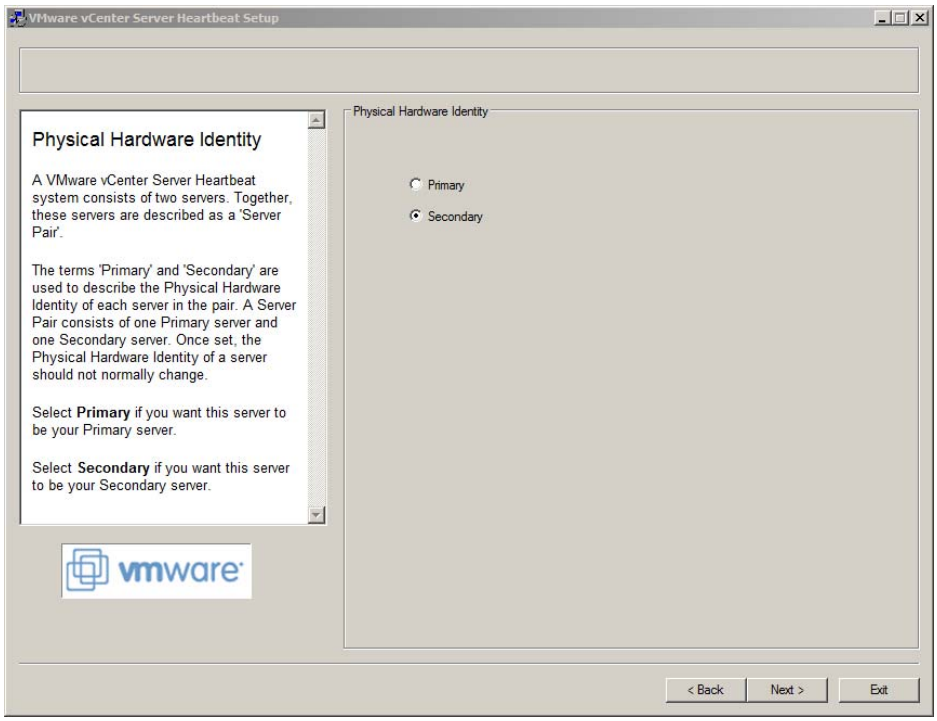


3 The **Setup Type** page is displayed. As with the installation on the Primary server, select **Install VMware vCenter Server Heartbeat** and click **Next**.


VMware vCenter Server Heartbeat Setup
Setup Type
Select the desired Setup type.
NOTE: before installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, please read any documentation that was supplied with the software and search VMware Knowledge Base, in particular for vCSHB Ref: 435.
NOTE: when installing or uninstalling a VMware vCenter Server Heartbeat component or Service Pack, you must use the most recent version of this Setup utility.
Select Install VMware vCenter Server Heartbeat to install the full VMware vCenter Server software suite on a Primary or Secondary server
Setup Type
Install VMware vCenter Server Heartbeat
Install Client Tools Only
Install AM(X)
Install Service Pack
Uninstall
Uninstall Selected Components
vmware
neverfail
WWW.NEVERFAILGROUP.COM
PREDICT · PROTECT · PERFORM
vCenter Server Heartbeat is powered by Neverfail®, for more information click here
< Back
Next >
Exit

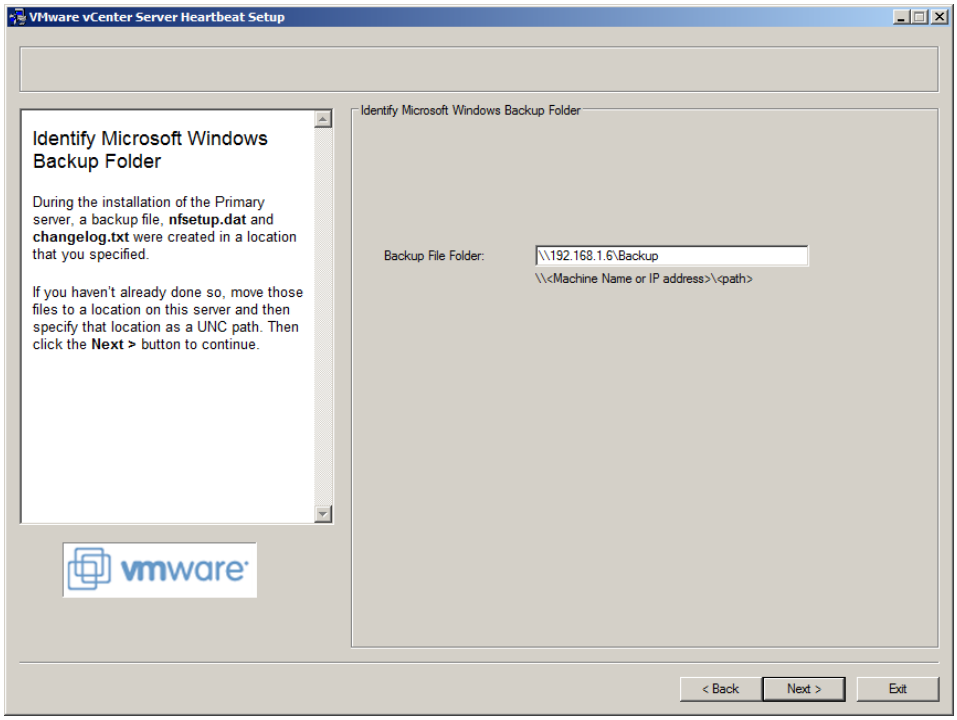
NOTE The left pane of each page in the setup wizard provides information about the setup process.

4 Select the identity of the server through the **Physical Hardware Identity** page. Select **Secondary** as the server identity and click **Next**.


VMware vCenter Server Heartbeat Setup
Physical Hardware Identity
A VMware vCenter Server Heartbeat system consists of two servers. Together, these servers are described as a 'Server Pair'.
The terms 'Primary' and 'Secondary' are used to describe the Physical Hardware Identity of each server in the pair. A Server Pair consists of one Primary server and one Secondary server. Once set, the Physical Hardware Identity of a server should not normally change.
Select Primary if you want this server to be your Primary server.
Select Secondary if you want this server to be your Secondary server.
Physical Hardware Identity
Primary
Secondary
vmware
< Back
Next >
Exit

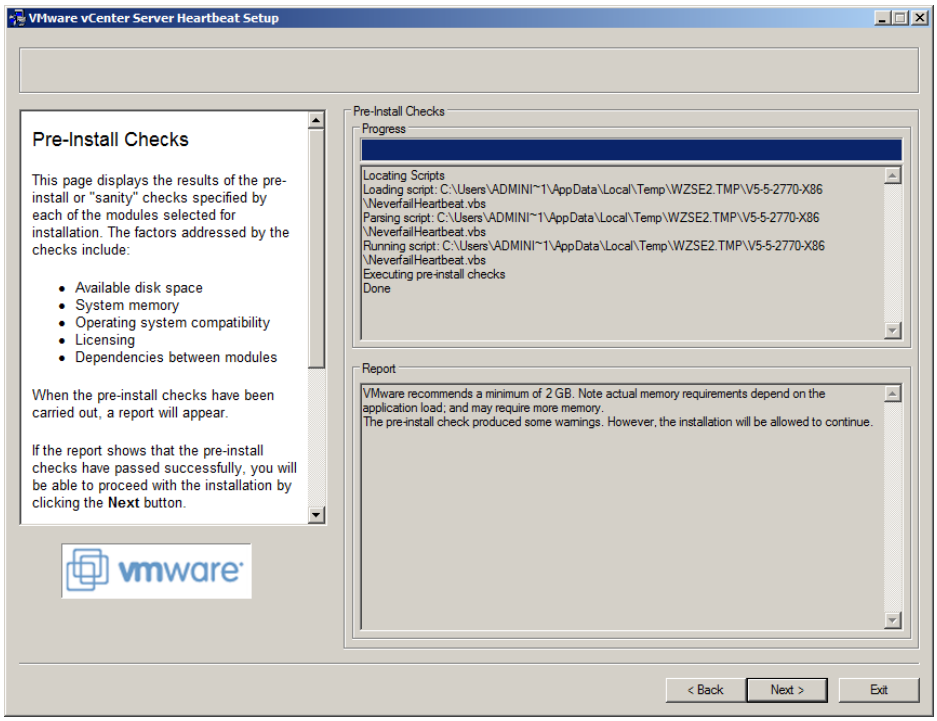
NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

5 Identify the location of the folder containing the backup file from the Primary server. Manually type the location path in the text box as a UNC path. Click **Next**.


VMware vCenter Server Heartbeat Setup
Identify Microsoft Windows Backup Folder
During the installation of the Primary server, a backup file, nfsetup.dat and changelog.txt were created in a location that you specified.
If you haven't already done so, move those files to a location on this server and then specify that location as a UNC path. Then click the Next > button to continue.
Identify Microsoft Windows Backup Folder
Backup File Folder:
\\192.168.1.6\Backup
\\<Machine Name or IP address>\<path>
vmware
< Back
Next >
Exit

6 The Pre-Install checks run. Click **Next**.

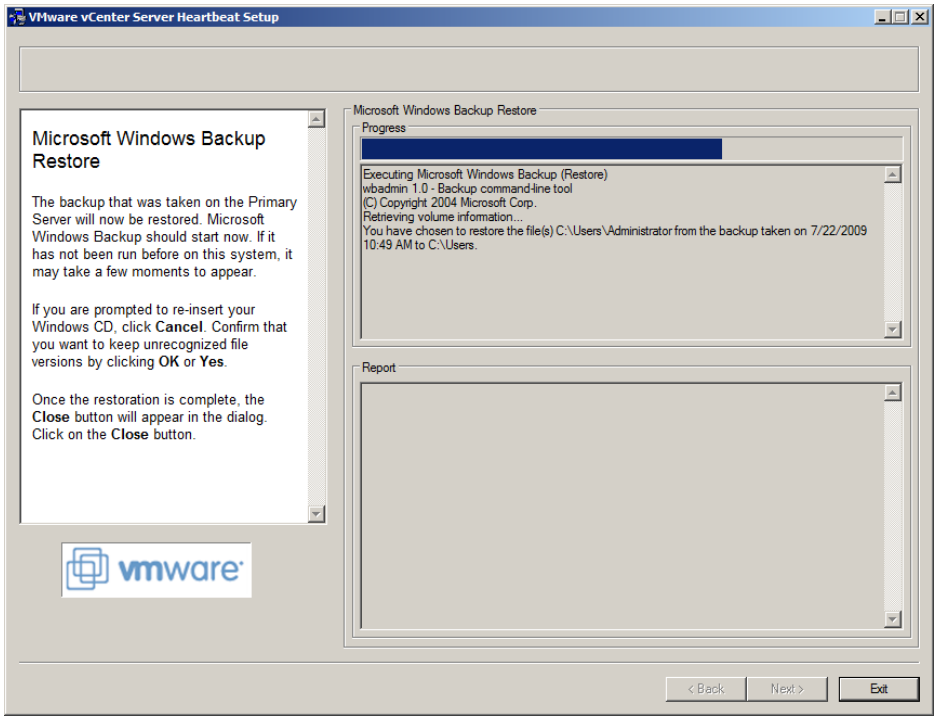
If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.


VMware vCenter Server Heartbeat Setup
Pre-Install Checks
This page displays the results of the pre-install or "sanity" checks specified by each of the modules selected for installation. The factors addressed by the checks include:
Available disk space
System memory
Operating system compatibility
Licensing
Dependencies between modules
When the pre-install checks have been carried out, a report will appear.
If the report shows that the pre-install checks have passed successfully, you will be able to proceed with the installation by clicking the Next button.
vmware
Pre-Install Checks
Progress
Locating Scripts
Loading script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Parsing script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Running script: C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\NeverfailHeartbeat.vbs
Executing pre-install checks
Done
Report
VMware recommends a minimum of 2 GB. Note actual memory requirements depend on the application load, and may require more memory.
The pre-install check produced some warnings. However, the installation will be allowed to continue.
< Back
Next >
Exit

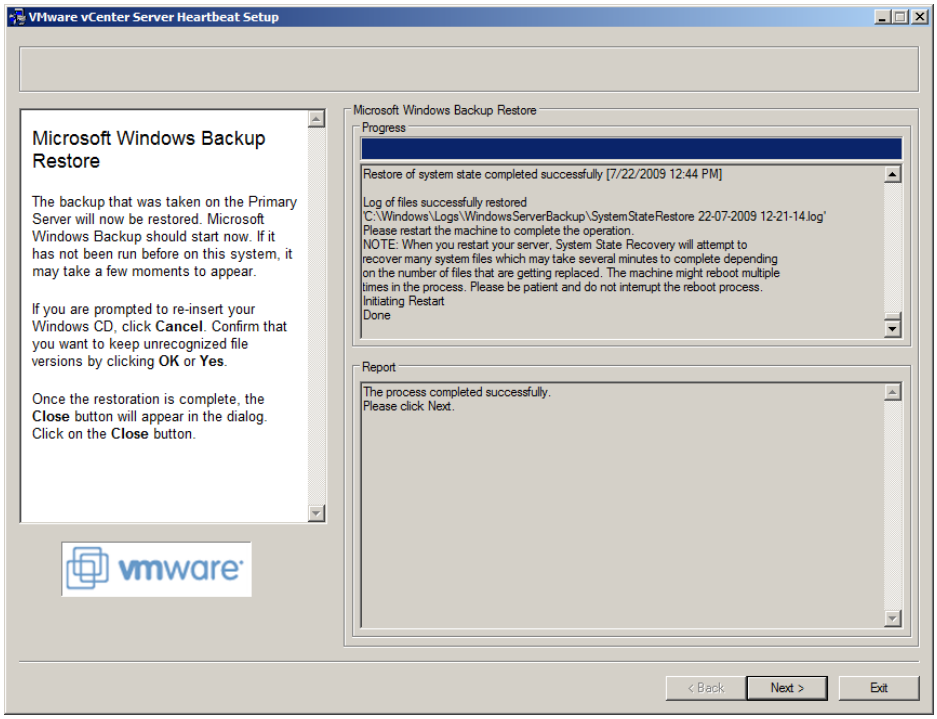
You have the following options:

- For installation using the Pre-Clone technique, go to Step 17 on page 100.
- For installation using the Install Clone technique, continue with Step 7.

7 The **Microsoft Windows Backup Restore** page is displayed. The **Microsoft Windows Backup Restore** page shows the progress of unbinding the packet filter and disabling NetBIOS from the channel NIC(s). After this process completes, a caution message advises you that the restore process is initiating and upon completion of the restore process, the server requires a restart. After restarting, Plug-and-Play (PnP) can require you to restart the machine more than once. Click **OK**.

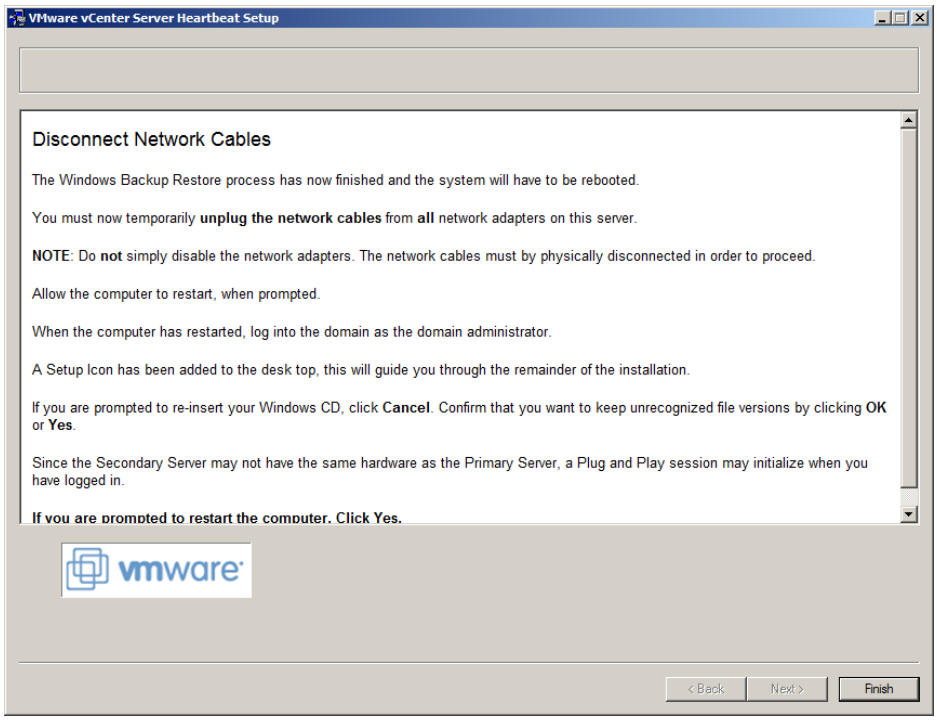

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Restore
The backup that was taken on the Primary Server will now be restored. Microsoft Windows Backup should start now. If it has not been run before on this system, it may take a few moments to appear.
If you are prompted to re-insert your Windows CD, click Cancel. Confirm that you want to keep unrecognized file versions by clicking OK or Yes.
Once the restoration is complete, the Close button will appear in the dialog. Click on the Close button.
vmware
Microsoft Windows Backup Restore
Progress
Executing Microsoft Windows Backup (Restore)
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.
Retrieving volume information...
You have chosen to restore the file(s) C:\Users\Administrator from the backup taken on 7/22/2009 10:49 AM to C:\Users.
Report
< Back
Next >
Exit

8 The progress of the backup restore is displayed in the Progress panel. When finished, a report on the restore is displayed in the Report panel. Review the backup restore report to verify successful completion. Click **Next**.

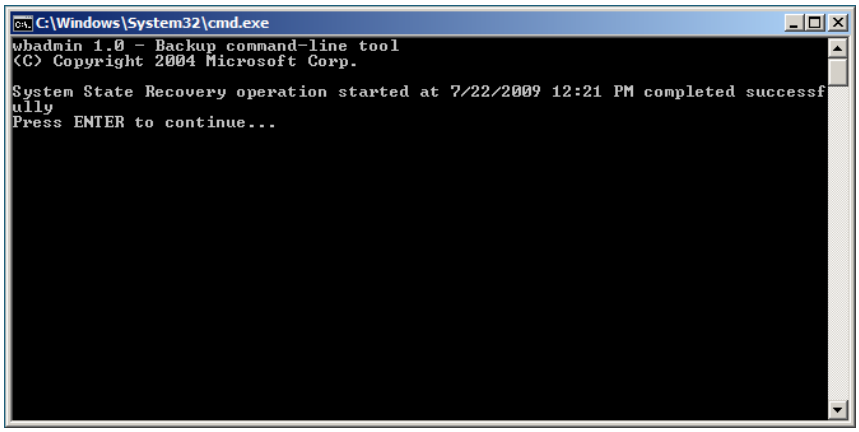

VMware vCenter Server Heartbeat Setup
Microsoft Windows Backup Restore
The backup that was taken on the Primary Server will now be restored. Microsoft Windows Backup should start now. If it has not been run before on this system, it may take a few moments to appear.
If you are prompted to re-insert your Windows CD, click Cancel. Confirm that you want to keep unrecognized file versions by clicking OK or Yes.
Once the restoration is complete, the Close button will appear in the dialog. Click on the Close button.
vmware
Microsoft Windows Backup Restore
Progress
Restore of system state completed successfully [7/22/2009 12:44 PM]
Log of files successfully restored
'C:\Windows\Logs\WindowsServerBackup\SystemStateRestore 22-07-2009 12-21-14.log'
Please restart the machine to complete the operation.
NOTE: When you restart your server, System State Recovery will attempt to recover many system files which may take several minutes to complete depending on the number of files that are getting replaced. The machine might reboot multiple times in the process. Please be patient and do not interrupt the reboot process.
Initiating Restart
Done
Report
The process completed successfully.
Please click Next.
< Back
Next >
Exit

9 The **Disconnect Network Cables** window is displayed. To disable the NICs is NOT sufficient. You must physically disconnect the network cables from the NICs. After disconnecting the network cables from the NICs, click **Finish**. A confirmation window is displayed. You must restart the machine to apply the newly restored System State. Click **Yes** to restart the server.

NOTE If this server is running in a virtual environment, disconnect the NICs from the virtual environment.


VMware vCenter Server Heartbeat Setup
Disconnect Network Cables
The Windows Backup Restore process has now finished and the system will have to be rebooted.
You must now temporarily unplug the network cables from all network adapters on this server.
NOTE: Do not simply disable the network adapters. The network cables must by physically disconnected in order to proceed.
Allow the computer to restart, when prompted.
When the computer has restarted, log into the domain as the domain administrator.
A Setup Icon has been added to the desk top, this will guide you through the remainder of the installation.
If you are prompted to re-insert your Windows CD, click Cancel. Confirm that you want to keep unrecognized file versions by clicking OK or Yes.
Since the Secondary Server may not have the same hardware as the Primary Server, a Plug and Play session may initialize when you have logged in.
If you are prompted to restart the computer, Click Yes.
vmware
< Back
Next >
Finish

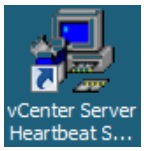
10 Following the restart of the server, a DOS window is presented stating that the restore of the System State was successful. Press Enter. Log in to the Secondary server using the domain administrator account. Click **Yes** at each restart prompt to allow each PnP cycle to complete.


C:\Windows\System32\cmd.exe
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.
System State Recovery operation started at 7/22/2009 12:21 PM completed successfully
Press ENTER to continue...

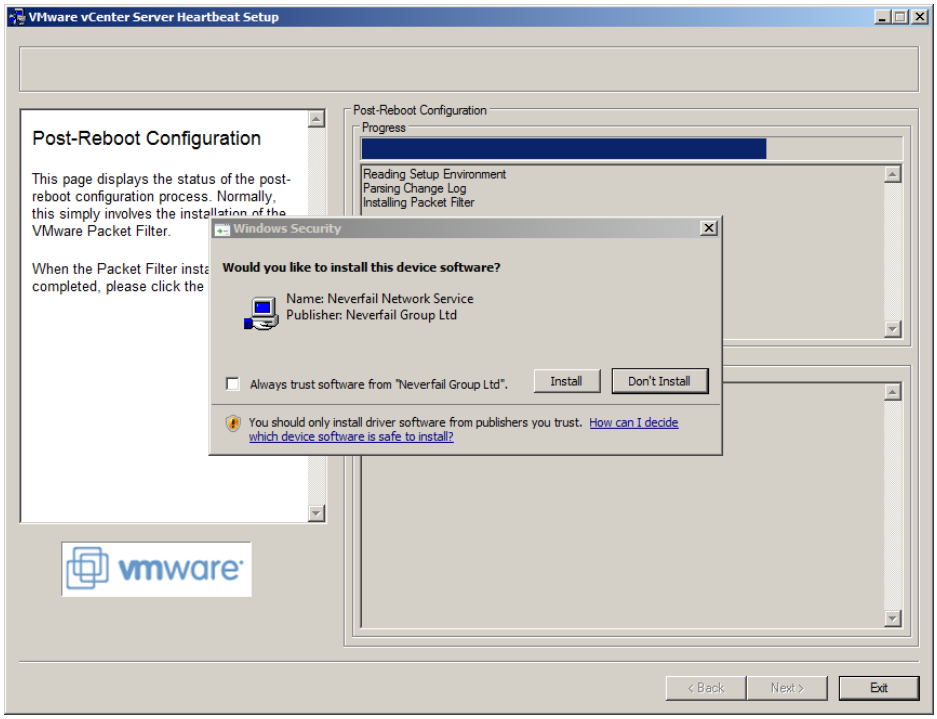
NOTE PnP can require multiple restarts of the server as it identifies the actual hardware makeup of the Secondary server as opposed to that restored from the backup file of the Primary server.

vCenter Server Heartbeat starts each time the Secondary server restarts. Manually shut down vCenter Server Heartbeat before initiating a restart.

11 After all PnP cycles complete, log in to the server and double-click the newly created **vCenter Server Heartbeat Setup Completion** icon created on the Desktop to continue the setup process.

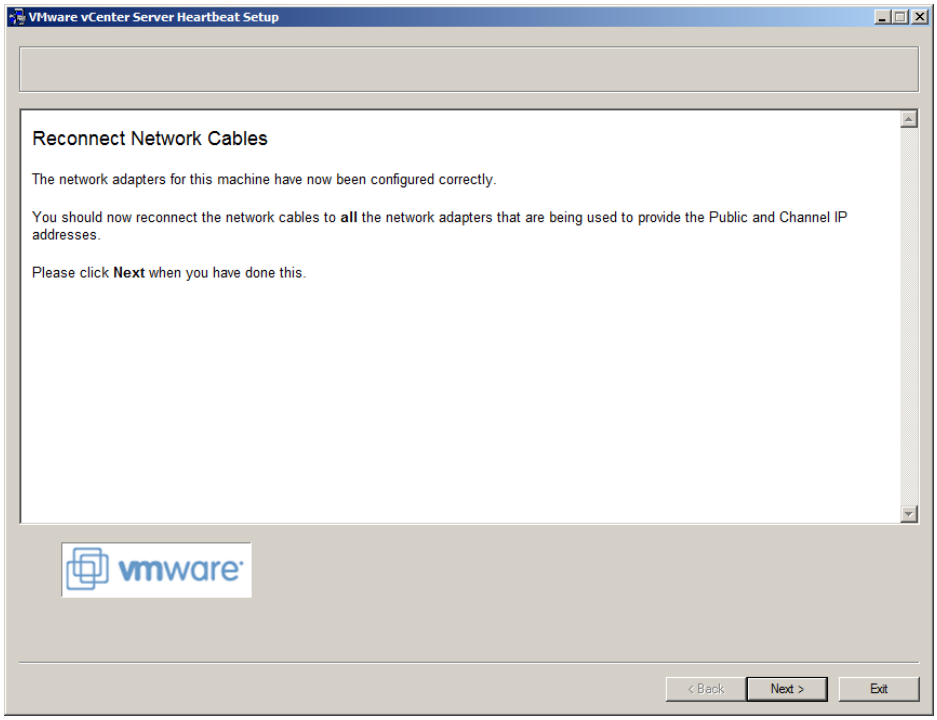


12 The **Post-Reboot Configuration** page is displayed. vCenter Server Heartbeat Setup installs the packet filter. When complete, click **Next**.

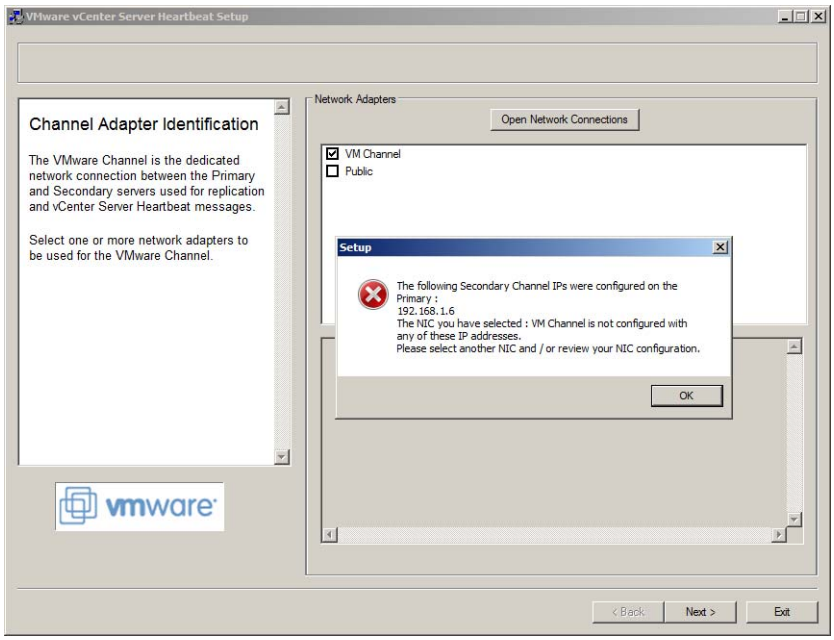

VMware vCenter Server Heartbeat Setup
Post-Reboot Configuration
This page displays the status of the post-reboot configuration process. Normally, this simply involves the installation of the VMware Packet Filter.
When the Packet Filter insta
completed, please click the
Post-Reboot Configuration
Progress
Reading Setup Environment
Parsing Change Log
Installing Packet Filter
Windows Security
Would you like to install this device software?
Name: Neverfail Network Service
Publisher: Neverfail Group Ltd
Always trust software from "Neverfail Group Ltd".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?
vmware
< Back
Next >
Exit

NOTE If you receive warnings that the driver is unsigned or did not complete the Windows Logo tests, click **Install**. If Windows is configured to display Signed Driver warnings, you can receive multiple warnings.

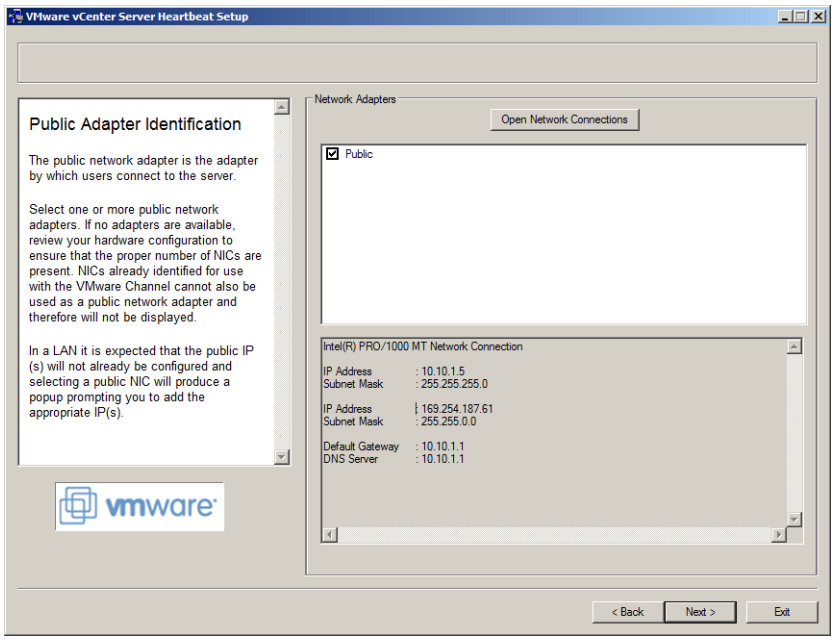
13 The **Reconnect Network Cables** window is displayed. Follow the instructions on this window to reconnect all of the previously disconnected network cables. After all network cables are connected, click **Next**.


VMware vCenter Server Heartbeat Setup
Reconnect Network Cables
The network adapters for this machine have now been configured correctly.
You should now reconnect the network cables to all the network adapters that are being used to provide the Public and Channel IP addresses.
Please click Next when you have done this.
vmware
< Back
Next >
Exit

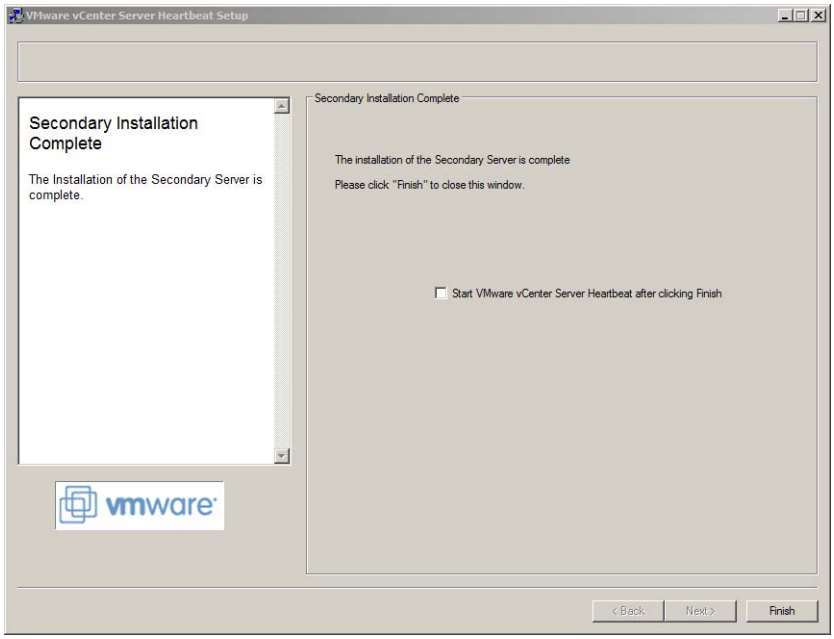
14 The **Channel Adapter Identification** page is displayed. Use this opportunity to reconfigure the VMware Channel NICs. During the cloning process, the IP address for the channel adapter on the Secondary server is reset to the IP address for the Primary server. To prevent network conflicts and to properly configure the VMware Channel, click **Open Network Connections** to display the network connections. Configure the Secondary Channel connection to the appropriate IP address (different from the IP address for the Primary Channel connection). After completing this configuration, select the check boxes for all Channel Connections and click **Next**.


VMware vCenter Server Heartbeat Setup
Channel Adapter Identification
The VMware Channel is the dedicated network connection between the Primary and Secondary servers used for replication and vCenter Server Heartbeat messages.
Select one or more network adapters to be used for the VMware Channel.
Network Adapters
Open Network Connections
VM Channel
Public
Setup
The following Secondary Channel IPs were configured on the Primary :
192.168.1.6
The NIC you have selected : VM Channel is not configured with any of these IP addresses.
Please select another NIC and / or review your NIC configuration.
OK
vmware
< Back
Next >
Exit

15 The **Public Adapter Identification** page is displayed. Select the Principal (Public) connection. Verify that the IP address configuration is correct.

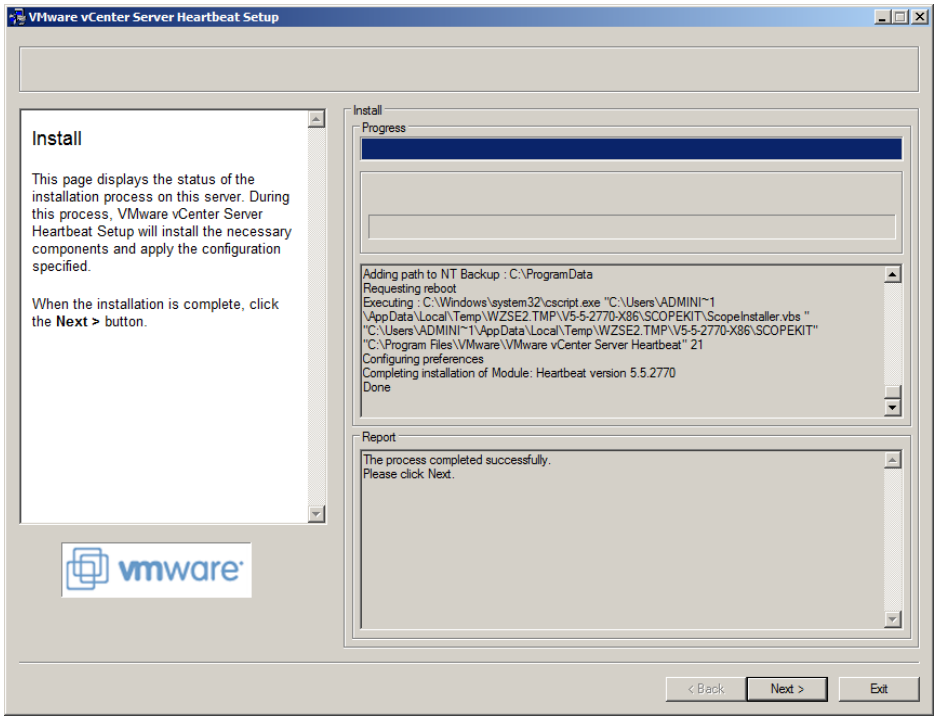

VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
In a LAN it is expected that the public IP (s) will not already be configured and selecting a public NIC will produce a popup prompting you to add the appropriate IP(s).
vmware
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
IP Address : 169.254.187.61
Subnet Mask : 255.255.0.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
< Back
Next >
Exit

16 The **Secondary Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**.

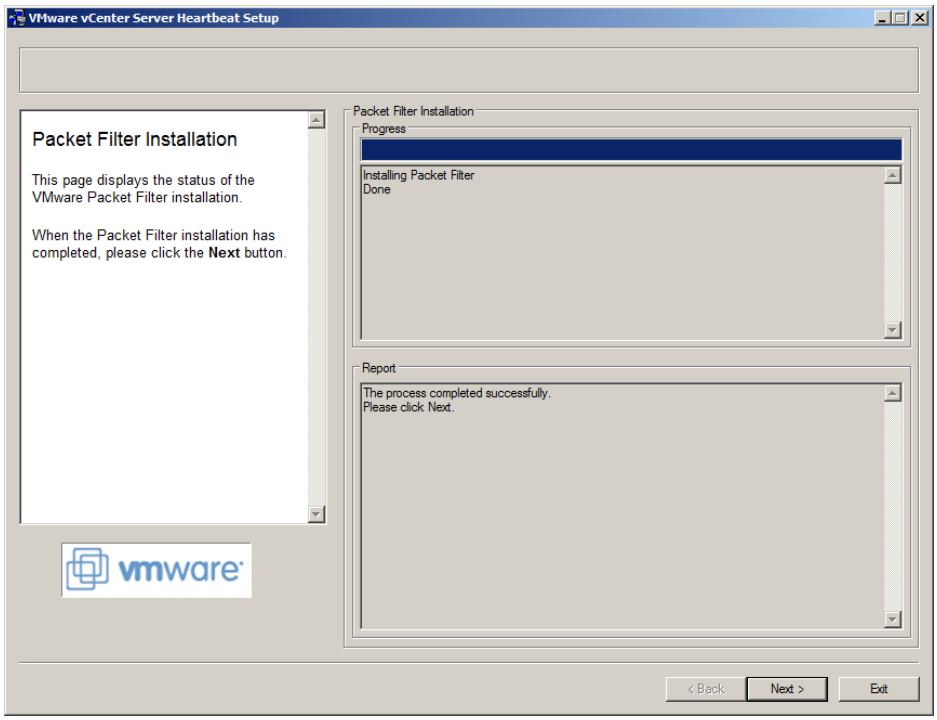

VMware vCenter Server Heartbeat Setup
Secondary Installation Complete
The Installation of the Secondary Server is complete.
vmware
Secondary Installation Complete
The installation of the Secondary Server is complete
Please click "Finish" to close this window.
Start VMware vCenter Server Heartbeat after clicking Finish
< Back
Next >
Finish

17 The next page displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and configures it with the default settings. To learn more about Heartbeat Diagnostics see *Getting Started with Heartbeat Diagnostics*.

18 The Report panel displays the results of the installation. Click **Next**.


VMware vCenter Server Heartbeat Setup
Install
This page displays the status of the installation process on this server. During this process, VMware vCenter Server Heartbeat Setup will install the necessary components and apply the configuration specified.
When the installation is complete, click the Next > button.
vmware
Install
Progress
Adding path to NT Backup : C:\ProgramData
Requesting reboot
Executing : C:\Windows\system32\cscript.exe "C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\SCOPEKIT\ScopeInstaller.vbs " "C:\Users\ADMINI~1\AppData\Local\Temp\WZSE2.TMP\V5-5-2770-X86\SCOPEKIT" "C:\Program Files\VMware\VMware vCenter Server Heartbeat" 21
Configuring preferences
Completing installation of Module: Heartbeat version 5.5.2770
Done
Report
The process completed successfully.
Please click Next.
< Back
Next >
Exit

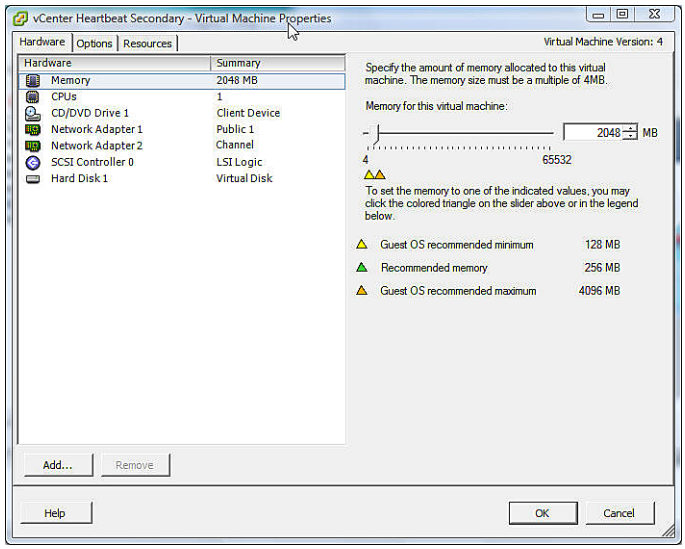
19 The progress of the VMware vCenter Server Heartbeat Packet Filter installation is displayed. Click **Next**.



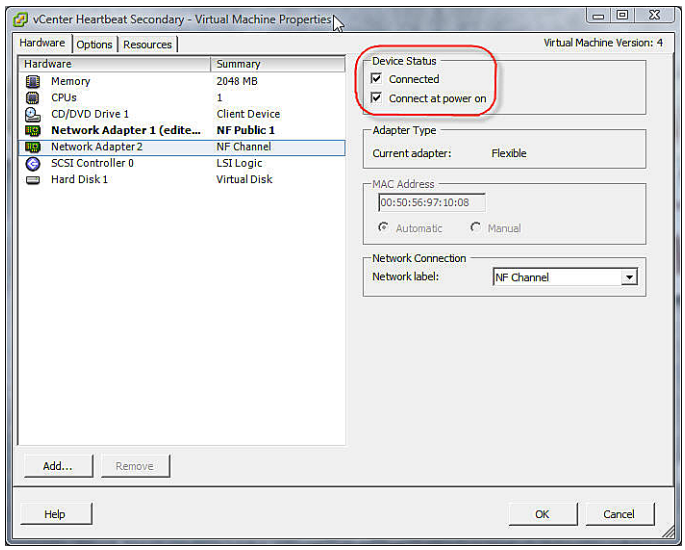
You have the following options:

- If the Secondary server is Physical such as in P2P, go to Step 23.
- If the Secondary server is Virtual such as in P2V or V2V, continue with Step a.

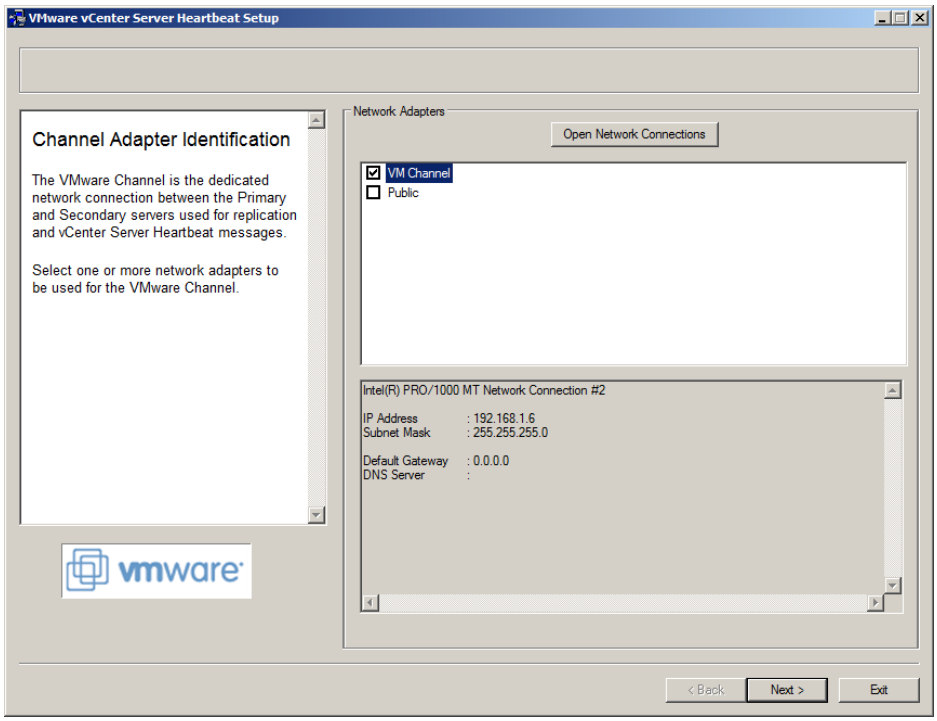
a The Packet Filter is installed on the Principal (Public) NIC and the Principal (Public) network adapter can be reconnected. Right-click the Secondary server image name and select **Edit Settings**.



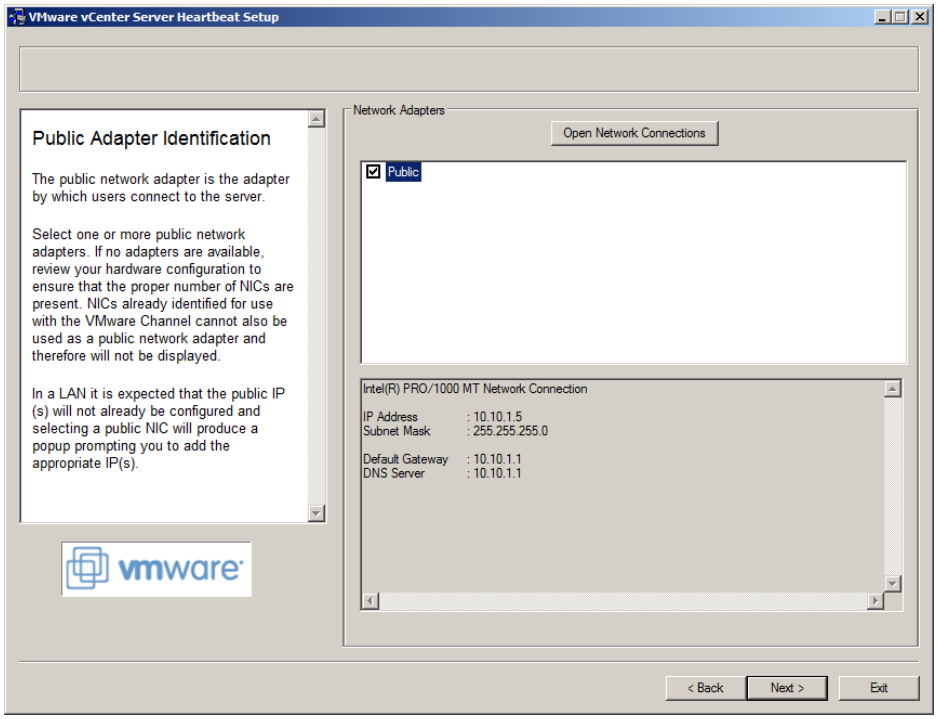
b Select the Principal (Public) virtual network adapter, select the **Connected** and **Connect at power on** check boxes, and click **OK**.



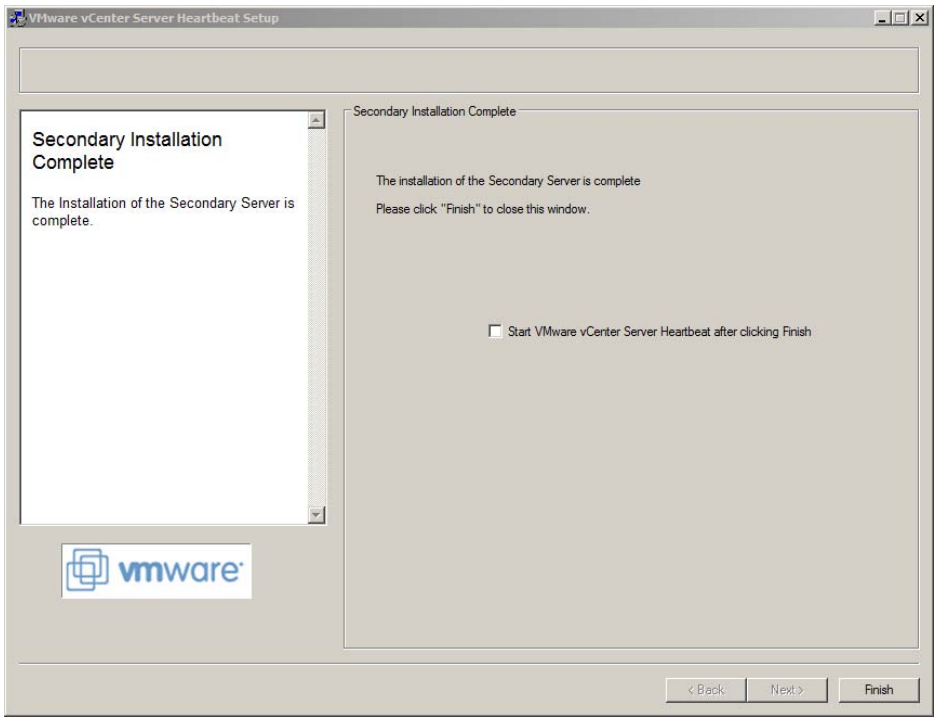
20 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower panel. Click **Next**.


VMware vCenter Server Heartbeat Setup
Channel Adapter Identification
The VMware Channel is the dedicated network connection between the Primary and Secondary servers used for replication and vCenter Server Heartbeat messages.
Select one or more network adapters to be used for the VMware Channel.
Network Adapters
Open Network Connections
VM Channel
Public
Intel(R) PRO/1000 MT Network Connection #2
IP Address : 192.168.1.6
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
DNS Server :
vmware
< Back
Next >
Exit

21 Configure the Principal (Public) adapter on the Secondary server through the **Public Adapter Identification** page. When you select the Principal (Public) adapter, a caution message notifies you that the IP address on the Principal (Public) adapter does not match the IP address on the Primary server (LAN configuration only).


VMware vCenter Server Heartbeat Setup
Public Adapter Identification
The public network adapter is the adapter by which users connect to the server.
Select one or more public network adapters. If no adapters are available, review your hardware configuration to ensure that the proper number of NICs are present. NICs already identified for use with the VMware Channel cannot also be used as a public network adapter and therefore will not be displayed.
In a LAN it is expected that the public IP (s) will not already be configured and selecting a public NIC will produce a popup prompting you to add the appropriate IP(s).
Network Adapters
Open Network Connections
Public
Intel(R) PRO/1000 MT Network Connection
IP Address : 10.10.1.5
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1
DNS Server : 10.10.1.1
vmware
< Back
Next >
Exit

22 The **Secondary Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**.


VMware vCenter Server Heartbeat Setup
Secondary Installation Complete
The Installation of the Secondary Server is complete.
Secondary Installation Complete
The installation of the Secondary Server is complete
Please click "Finish" to close this window.
Start VMware vCenter Server Heartbeat after clicking Finish
vmware
< Back
Next >
Finish

23 Before starting vCenter Server Heartbeat, verify the time synchronization between the Primary and Secondary servers. When a difference exists, synchronize the Secondary (passive) server to the Primary (active) server across the VMware Channel. Type the following command at the command prompt:

```
net time \\<Primary_Channel_IP_address> /set
```

Start vCenter Server Heartbeat on the Primary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icons change from a double dash to a **P**, indicating the server is the Primary server, and an **A** indicating the server is acting in an active role.

Start vCenter Server Heartbeat on the Secondary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icon changes from a double dash to an **S**, indicating that the server is the Secondary server, and a dash (–), indicating that the server is in a passive role.

24 The Primary and Secondary servers establish a handshake and commence replication.

NOTE The installation is complete if vCenter Server was installed with a local SQL Server or only vCenter Server was installed with no separate SQL Server.

If vCenter Server only was installed and you want to install a separate SQL Server, repeat the installation process for the Primary and Secondary servers at the remote site and select **SQL Server only**.

To install SQL Server on a separate host from the vCenter Server, go to "Primary Server" on page 72.

25 Configure the appropriate username and password in the vCenter Server Heartbeat Console:

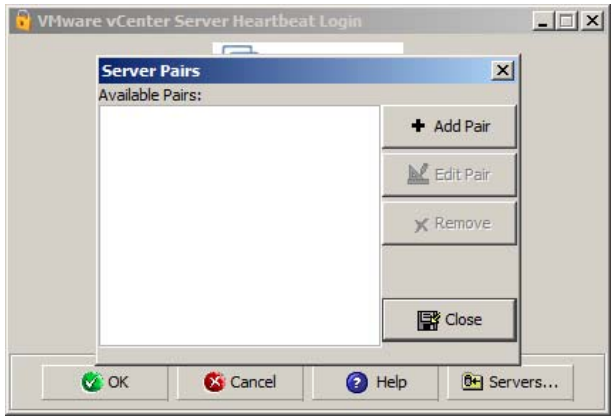
a Start vCenter Server Heartbeat Console from the desktop shortcut or **Start** > **All Programs** > **VMware** > **VMware vCenter Server Heartbeat** > **Manage Server**. The login page is displayed.

b Before you log in, you must identify the pair of servers to administer. Click **Servers**.

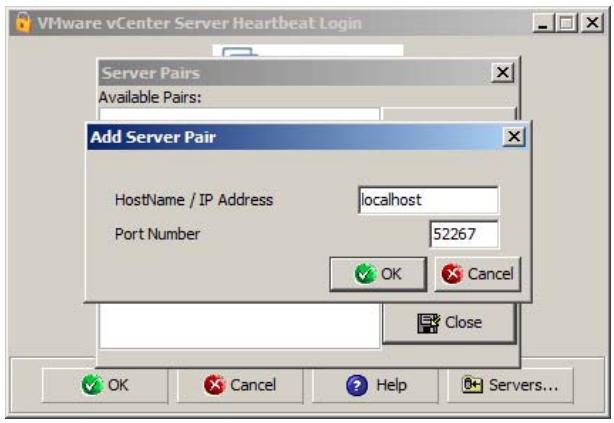
NOTE It is recommended that you add the Principal (Public) IP address or the Fully Qualified Domain Name of the Primary server to ensure that you can administer the pair from the vCenter Server Heartbeat Console regardless of whether the current server role is active or passive.

---

c Click **Add Pair**.



d Type the IP address of any NIC on the active server or the NetBIOS name of the server pair and click **OK**.



e The server pair appears in the list. If more than one server pair exists within the organization, add them sequentially to the list by repeating the procedure.

To edit or delete server pairs from the list, click the entry in the list and click the relevant button.

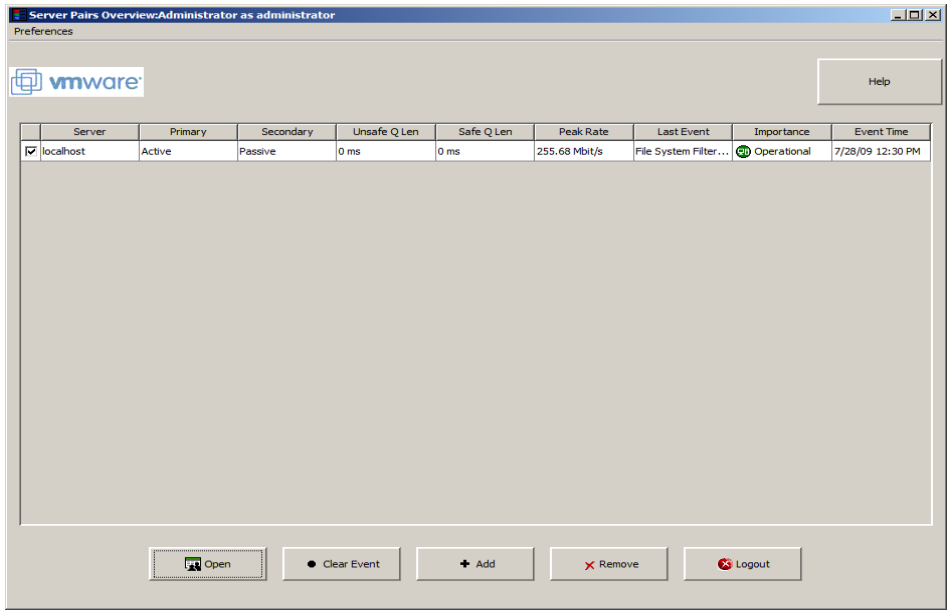
f Click **Close** to return to the login window.

To administer a pair of servers you must connect to them through the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes. Wait 10 seconds after starting vCenter Server Heartbeat before attempting to connect.

g Select a server pair in the Server list.

h Type a username and password with valid Windows credentials. In a domain environment, use the format **`domainname\username`**.

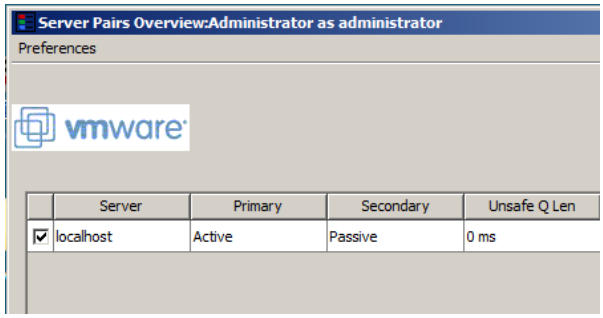
i The **Server Pairs Overview** window lists the selected pair of servers with other server pairs that historically were administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.



Additionally, the **Last Event**, **Importance**, and **Event Time** data are displayed. These events are discussed later in this guide.

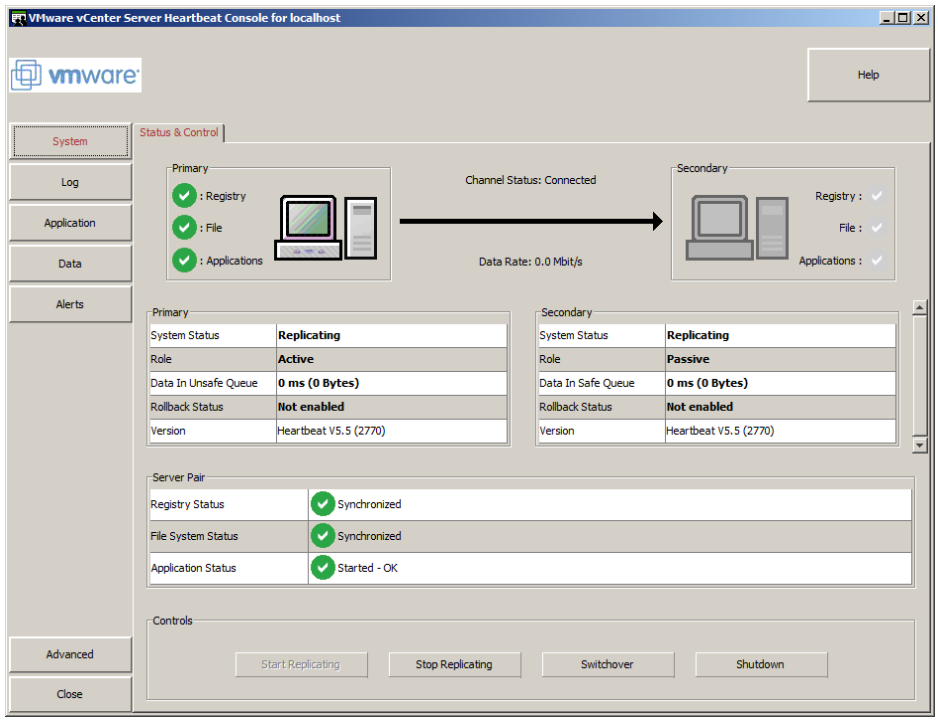
j To add additional pairs of servers, click **Add** and follow the previously described procedure.

k To select a pair listed in the main data grid, select the check box next to the server name.

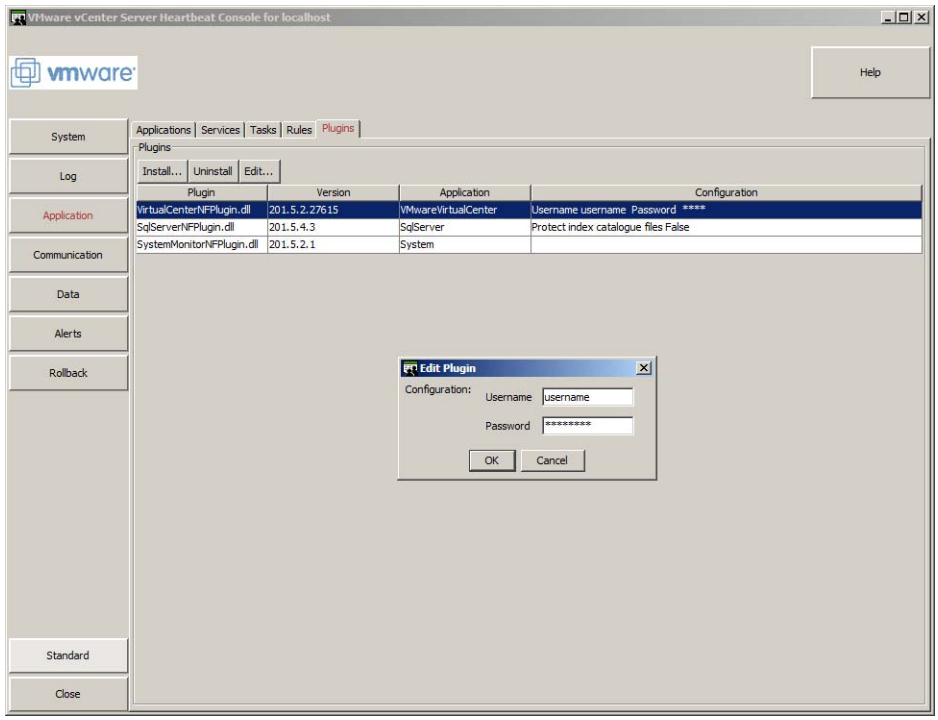


l When a pair is selected, the **Open**, **Clear Event**, and **Remove** buttons become active.

m **Open** displays the pair of servers for administration and configuration and displays the **System** > **Status and Control** page.



n Click **Advanced** > **Application** > **Plugins**.



o Select the vCenter Server plug-in.

p Click **Edit**.

q Type the username and password for an account with rights to the virtual infrastructure.

r Click **OK**.

Post Installation Configuration

Upon completion of installation, a series of tasks must be performed to ensure that vCenter Server Heartbeat is properly configured.

Add the VMware License

After completion of installation, vCenter Server Heartbeat will run in the evaluation mode for up to 60 days. After acquiring a license, you must add the VMware vCenter Server Heartbeat license using the Configure Server wizard to change from evaluation mode to production mode. To add the license:

1 Right-click the **System Tray** icon and select **Stop VMware vCenter Server Heartbeat** opting to leave protected applications running.

2 Double-click the **Configure Server** icon on the desktop.

3 Select the **License** tab of the Configure Server wizard.

4 Select the existing license and click the **Trash Can** icon.

5 Click the **Add Row** icon and enter the VMware vCenter Server Heartbeat license key.

6 Click **Finish**.

7 Right-click the **System Tray** icon and select **Start VMware vCenter Server Heartbeat**.

When Deployed in a WAN Environment

When deployed in a WAN environment with VMware Orchestrator and the Primary and Secondary servers in different subnets, you must configure an Exclusion File Filter following the steps below:

1 Launch **vCenter Server Heartbeat Console**.

2 Click **Advanced** to enable Advanced mode view.

3 Click **Data** and select the **Configuration** tab.

4 Click **Add Exclusion Filter...** and type the following path:

```
$INSTALL_PATH_TO_ORCHESTRATOR/app-server/bin/boot.properties
```

5 Click **OK.**

6 Perform a switchover so that the Secondary server becomes active.

7 Launch the **vCenter Orchestrator Web Configuration** wizard and select **Network**. In the **IP address** field select the Principal (Public) IP address of the Secondary server. Click **Apply changes**.

8 Start the vCenter Orchestrator Web Configuration Wizard from the Start menu: **Start** > **Programs** > **VMware** > **Startup Options**, click **Install vCO server as service**, and click **Start service**.

9 Launch the **vCenter Orchestrator Web Configuration** wizard, select **Startup Options**, and click **Restart service**.

10 From **vCenter Server Heartbeat Console**, select **Application** and then **Services**. Verify that **VMware vCenter Orchestrator Server** service is included in the protected services. If not, manually run the **Protected Service Discovery** task from **VMware vCenter Heartbeat Console** > **Application** > **Tasks** > **VMware VirtualCenter - Protected Service Discovery**)

vCenter Server 2.5

The post installation configuration tasks are determined by the type of network environment.

LAN

For LAN deployments, perform the following:

1 If a Management IP address is configured, no additional tasks are required.

2 If a Management IP address is not configured, configure a VMware Managed IP address using the Virtual Infrastructure Client.

   a Launch the Virtual Infrastructure Client.

   b In the Virtual Infrastructure Client, navigate to **Administration** > **VirtualCenter Management Server Configuration** > **Runtime Settings**.

   c In the Managed IP field, type the Principal (Public) IP address.

   d Click **OK** and close the window.

WAN

For WAN deployments, regardless of whether a Management IP address exists, vCenter Server Heartbeat provides a task that can be configured to update the ESX hosts with the new Managed IP address during a switchover or failover. The task requires setting the Managed IP in either in the `vpxd.cfg` file or in the registry.

To configure the Managed IP in the Vpxd file

1 The `vpxd.cfg` file is located at `C:\Documents and Settings\All Users\Application Data\VMware\VMware Virtual Center server`.

2 On the active server, locate the `<vpxd>` element in the `vpxd.cfg` file and add a new element `<managedIP>` that contains the Principal (Public) IP address of the vCenter server.

To configure the Managed IP in the registry

At `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VirtualCenter`, create a new string value called `<managedIP>` and set it with the Public (Principal) IP address of the currently active server.

IMPORTANT Do not configure the VMware Managed IP address using the Virtual Infrastructure Client. The Managed IP field from **Administration** > **VirtualCenter Management Server Configuration** > **Runtime Settings** must be clear.

---

vCenter Server 4.0

The post installation configuration tasks are determined by the type of network environment.

LAN

With or without a Management IP address configured, no additional tasks are required.

WAN

With or without a Management IP address configured, disable the **VMware VirtualCenter PostStart** task through the vCenter Server Heartbeat Console using the following procedure.

1 Launch the vCenter Server Heartbeat Console.

2 Click **Application**.

3 Select the **Tasks** tab.

4 Select **VMware VirtualCenter PostStart** task.

5 Click **Edit**.

6 Clear the **Enabled** check box.

7 Click **OK**.

IMPORTANT Do not configure the Managed IP address using the vSphere Client. The vCenter Server Managed IP field from **Administration** > **vCenter Server Settings** > **Runtime Settings** must be clear.

Configuring vCenter Server Heartbeat 5

This chapter includes the following topics:

- "Server Configuration Wizard" on page 114
- "Configuring the Machine Identity" on page 115
- "Configuring the Server Role" on page 115
- "Configuring the Client Connection Port" on page 115
- "Configuring Channel IP Routing" on page 115
- "Configuring the Default Channel Port" on page 116
- "Configuring Low Bandwidth Module" on page 116
- "Configuring Public IP Addressing" on page 116
- "Enabling Network Monitoring" on page 117
- "Configuring Split-Brain Avoidance" on page 118
- "Managing vCenter Server Heartbeat License Keys" on page 119
- "Configuring the Maximum Disk Usage" on page 120

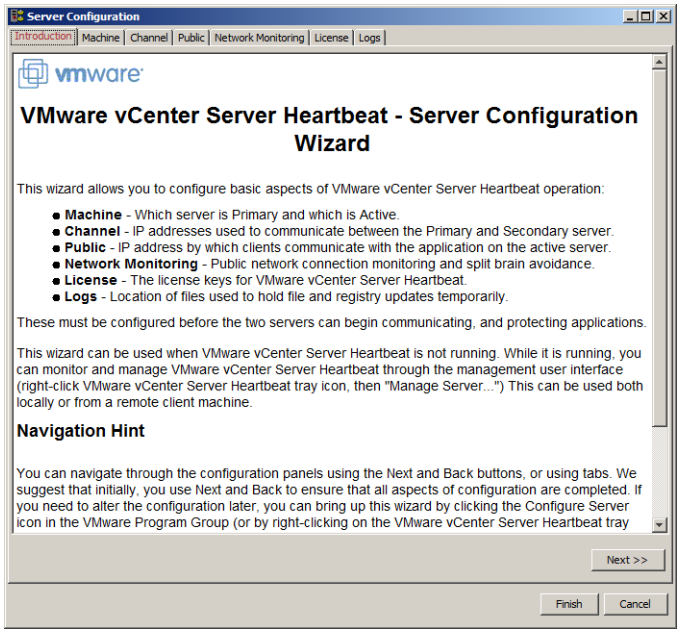
Server Configuration Wizard

The **VMware vCenter Server Heartbeat – Server Configuration Wizard** (Configure Server wizard) sets up and maintains communications between the vCenter Server Heartbeat servers. Configuration information includes the IP address for the VMware Channel(s) and Principal (Public) addresses on both servers.

After the system is set up and is functioning correctly, you do not need to reconfigure the system. The Configure Server wizard becomes redundant during daily operations of the software.

1 Before launching the Configure Server wizard to change the vCenter Server Heartbeat configuration, you must stop vCenter Server Heartbeat.

2 Click the Configure Server icon on the desktop or **Start** > **All Programs** > **VMware** > **VMware vCenter Server Heartbeat** > **Configure Server** to launch the Configure Server wizard.


Server Configuration
Introduction
Machine
Channel
Public
Network Monitoring
License
Logs
vmware
VMware vCenter Server Heartbeat - Server Configuration Wizard
This wizard allows you to configure basic aspects of VMware vCenter Server Heartbeat operation:
Machine - Which server is Primary and which is Active.
Channel - IP addresses used to communicate between the Primary and Secondary server.
Public - IP address by which clients communicate with the application on the active server.
Network Monitoring - Public network connection monitoring and split brain avoidance.
License - The license keys for VMware vCenter Server Heartbeat.
Logs - Location of files used to hold file and registry updates temporarily.
These must be configured before the two servers can begin communicating, and protecting applications.
This wizard can be used when VMware vCenter Server Heartbeat is not running. While it is running, you can monitor and manage VMware vCenter Server Heartbeat through the management user interface (right-click VMware vCenter Server Heartbeat tray icon, then "Manage Server...") This can be used both locally or from a remote client machine.
Navigation Hint
You can navigate through the configuration panels using the Next and Back buttons, or using tabs. We suggest that initially, you use Next and Back to ensure that all aspects of configuration are completed. If you need to alter the configuration later, you can bring up this wizard by clicking the Configure Server icon in the VMware Program Group (or by right-clicking on the VMware vCenter Server Heartbeat tray
Next >>
Finish
Cancel

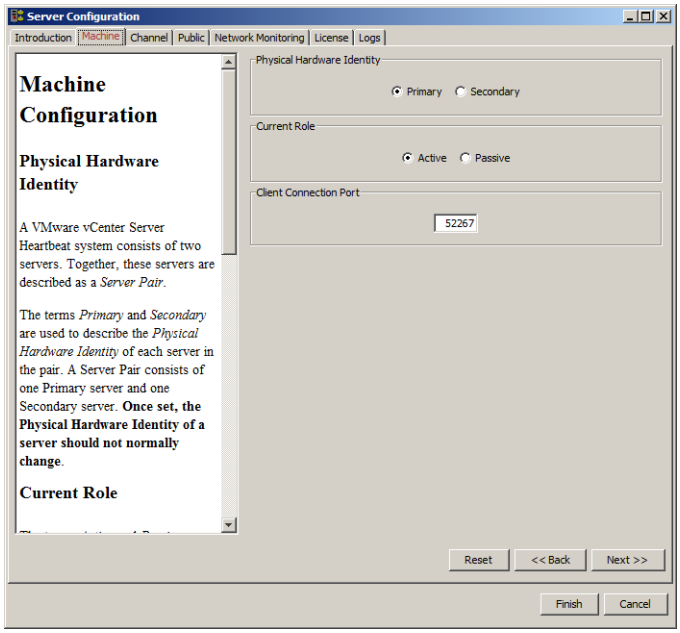
Configuring the Machine Identity

CAUTION The machine Identity should only be changed when directed to do so by VMware Support or when instructed to by a knowledge base article. vCenter Server Heartbeat is designed not to allow two passive or two active servers to connect.

To change the machine identity

1 Click the **Machine** tab and select a **Physical Hardware Identity** for the local machine.

2 Click **Next** or **Finish**.



Configuring the Server Role

To change the server role, click the **Machine** tab, select the **Current Role** of the local machine, and click **Next** or **Finish**.

NOTE Before changing the role of the local server, verify that the other (remote) server in the pair is not already performing the same role.

Configuring the Client Connection Port

Clients such as the vCenter Server Heartbeat Console use the Client Connection Port to connect to vCenter Server Heartbeat. Do not change this port unless another application is using it. To change the Client Connection Port, click the **Machine** tab, edit the default entry (52267) and click **Next** or **Finish**.

Configuring Channel IP Routing

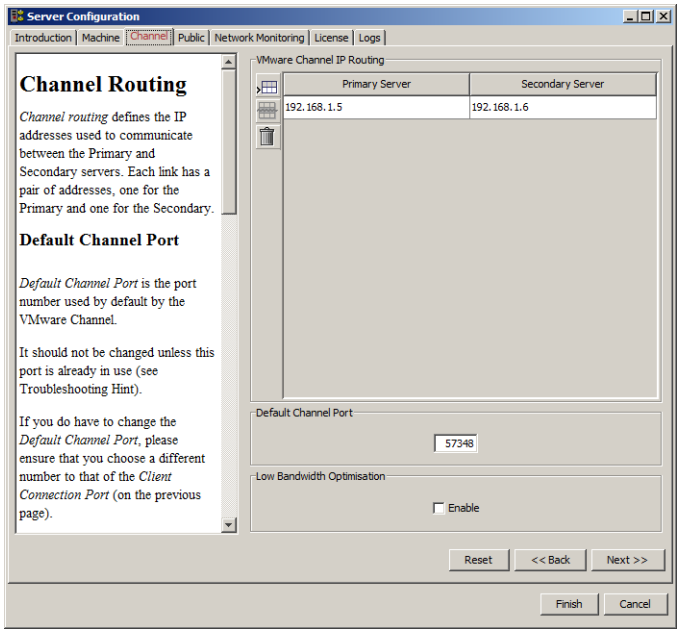
Channel IP routing defines the IP addresses used to communicate between the Primary and Secondary servers. Each link has a pair of addresses, one for the Primary, and one for the Secondary.

To add an additional VMware Channel after installing the NICs and configuring them

1 Click the **Channel** tab. Click **Add Row** to add the new IP addresses for both the Primary and Secondary server to the VMware Channel IP Routing table.

2 Use the drop-down menu to view a list of available IP addresses on the local server.

3 Type the remote server IP address.


Server Configuration
Introduction
Machine
Channel
Public
Network Monitoring
License
Logs
Channel Routing
Channel routing defines the IP addresses used to communicate between the Primary and Secondary servers. Each link has a pair of addresses, one for the Primary and one for the Secondary.
Default Channel Port
Default Channel Port is the port number used by default by the VMware Channel.
It should not be changed unless this port is already in use (see Troubleshooting Hint).
If you do have to change the Default Channel Port, please ensure that you choose a different number to that of the Client Connection Port (on the previous page).
VMware Channel IP Routing
Primary Server
Secondary Server
192.168.1.5
192.168.1.6
Default Channel Port
57348
Low Bandwidth Optimisation
Enable
Reset
<< Back
Next >>
Finish
Cancel

4 To change the VMware Channel IP addresses, select and edit the entry in the table.

5 Click **Next** or **Finish**.

Configuring the Default Channel Port

VMware Channel uses the Default Channel Port to communicate between the Primary and Secondary server. Do not change this port unless another application is using it. To change the Default Channel Port, click the **Channel** tab, edit the default entry (57348), and click **Next** or **Finish**.

Configuring Low Bandwidth Module

This feature is enabled during installation. To disable this feature, click the **Channel** tab and clear the Low Bandwidth Optimization check box. When enabled, the VMware Channel optimizes communications for low bandwidth connections. Low Bandwidth Optimization (LBO) stores data on disk rather than in memory and is essential for WAN installations or when bandwidth is limited.

To enable LBO, click the **Channel** tab, select the check box to enable the feature and click **Next** or **Finish**.

NOTE This feature is designed for implementations where the available throughput on the VMware Channel is slower than 10 Mbit/s. Do not enable the Low Bandwidth Module in a LAN, this feature is not designed to work in a LAN where the throughput is much faster.

Configuring Public IP Addressing

vCenter Server Heartbeat servers are configured with one or more Principal (Public) IP addresses. These are the addresses used by clients of the protected application to connect to the application. Typically, there is one Principal (Public) IP address.

You must configure all of the Principal (Public) IP addresses on both Primary and Secondary servers. On the passive server, all traffic to and from these Principal (Public) IP addresses is blocked. On the active server, all traffic passes through. When the server roles switch, the IP filtering mode also switches, so client systems always connect to the Principal (Public) IP addresses on the server that is currently active. When the vCenter Server Heartbeat service shuts down, the filtering remains in place so no IP address conflicts occur between the two servers.

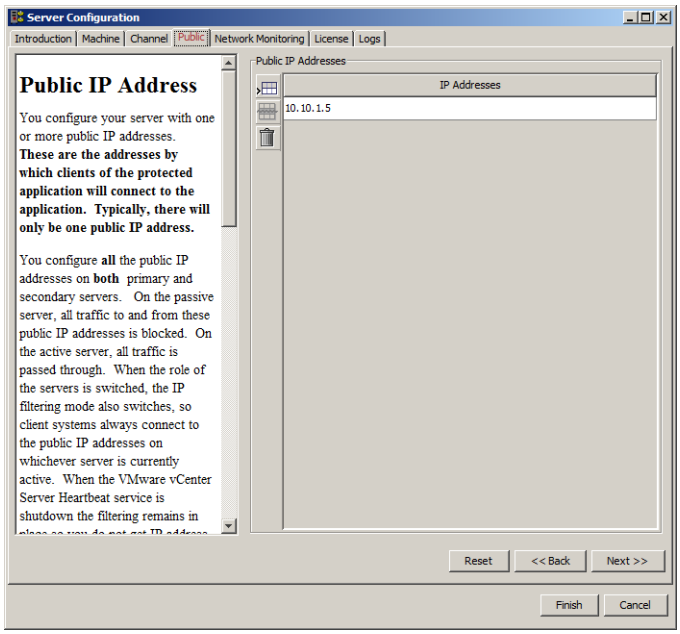
To configure Principal (Public) IP address

1 Click the **Public** tab and list all the addresses used as Principal (Public) IP addresses.

An address must not appear more than once. The Principal (Public) IP addresses listed cannot be the same as any of the IP addresses listed in the **Channel** tab.

2 To add an address, double-click a row and type in the address or select it from a list of currently defined addresses.

3 Click **Next** or **Finish**.


Server Configuration
Introduction
Machine
Channel
Public
Network Monitoring
License
Logs
Public IP Address
You configure your server with one or more public IP addresses. These are the addresses by which clients of the protected application will connect to the application. Typically, there will only be one public IP address.
You configure all the public IP addresses on both primary and secondary servers. On the passive server, all traffic to and from these public IP addresses is blocked. On the active server, all traffic is passed through. When the role of the servers is switched, the IP filtering mode also switches, so client systems always connect to the public IP addresses on whichever server is currently active. When the VMware vCenter Server Heartbeat service is shutdown the filtering remains in
Public IP Addresses
IP Addresses
10.10.1.5
Reset
<< Back
Next >>
Finish
Cancel

Enabling Network Monitoring

vCenter Server Heartbeat can monitor the connection between the active server and the Principal (Public) network. VMware recommends that you enable this feature.

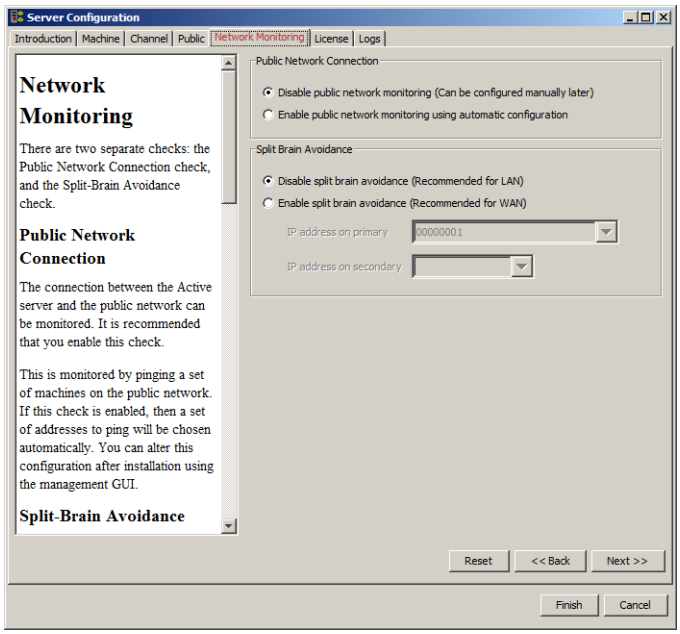
The network is monitored by pinging a set of machines on the Principal (Public) network. If enabled, the system routinely pings a set of default set of addresses. Use the vCenter Server Heartbeat Console to change the configuration after installation.

To enable Network Monitoring

1 Click the **Network Monitoring** tab.

2 Select **Enable public network monitoring using automatic configuration**.

3 Click **Next** or **Finish**.


Server Configuration
Introduction
Machine
Channel
Public
Network Monitoring
License
Logs
Network Monitoring
There are two separate checks: the Public Network Connection check, and the Split-Brain Avoidance check.
Public Network Connection
The connection between the Active server and the public network can be monitored. It is recommended that you enable this check.
This is monitored by pinging a set of machines on the public network. If this check is enabled, then a set of addresses to ping will be chosen automatically. You can alter this configuration after installation using the management GUI.
Split-Brain Avoidance
Public Network Connection
Disable public network monitoring (Can be configured manually later)
Enable public network monitoring using automatic configuration
Split Brain Avoidance
Disable split brain avoidance (Recommended for LAN)
Enable split brain avoidance (Recommended for WAN)
IP address on primary
00000001
IP address on secondary
Reset
<< Back
Next >>
Finish
Cancel

Configuring Split-Brain Avoidance

Split-brain Avoidance is used in WAN installations to ensure that only one server becomes active if the VMware Channel connection is lost, but both servers are still connected to the Principal (Public) network.

Split-brain Avoidance works by pinging from the passive server to the active server across the Principal (Public) network. If the active server responds, the passive does not initiate failover, even if the VMware Channel connection is lost. This feature requires that the active and passive servers have different IP addresses on the Principal (Public) network, which is typical for WAN installations.

To enable this feature, click the **Network Monitoring** tab and select **Enable split brain avoidance (Recommended for WAN)**. Type the Principal (Public) IP address used by each server.

You must configure auxiliary IP addresses on both Principal (Public) network cards to allow the passive server to send a ping and send email alerts. Auxiliary IP addresses are additional IP addresses assigned to the network card, which is connected to the Principal (Public) network. They allow the passive server to communicate because unlike the Principal (Public) network address they are not filtered.

To configure an auxiliary IP address

1 Open the network properties for the Principal (Public) network connection.

2 Double-click **Internet Protocol (TCP/IP)** to display the properties.

3 Click **Advanced**.

4 Type an additional (currently unused) IP address in the table.

5 Reposition the IP addresses in the list so that the additional (auxiliary) IP address appears first and the Principal (Public) network address that clients use to connect to the server appears second.

NOTE You can reposition the IP addresses by deleting it at the top of the list and adding it at the bottom.

6 Click **OK** three times.

7 Click **Next** or **Finish**.

Managing vCenter Server Heartbeat License Keys

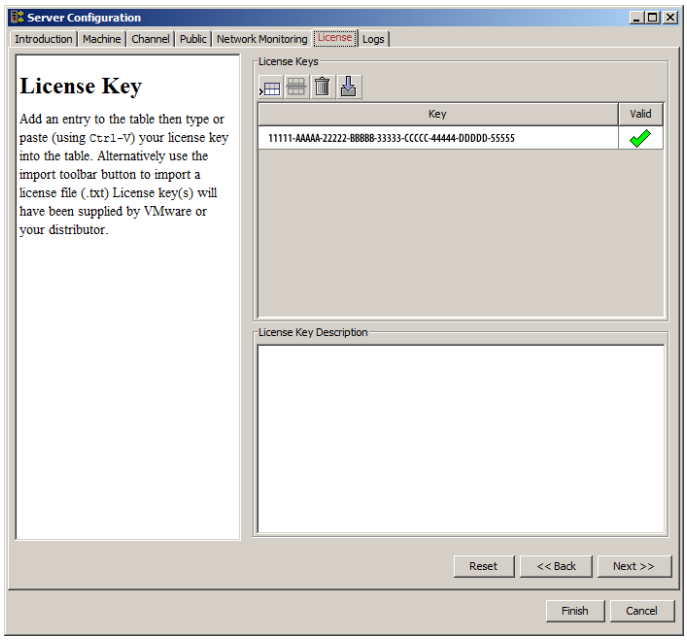
To manage vCenter Server Heartbeat license keys, select the *License* tab of the *Configure Server* wizard.

To add an entry to the License Keys table

1 Click the **Add Row** icon and enter your VMware vCenter Server Heartbeat serial number.

2 Manually type or paste (**using Ctrl-V**) your license key into the table.

3 Click **Next** or **Finish**.



Configuring Message Queue Logs

The server temporarily stores replication data received in the passive server (safe) queue and the replication data waiting in the active server (unsafe) queue in message queue logs.

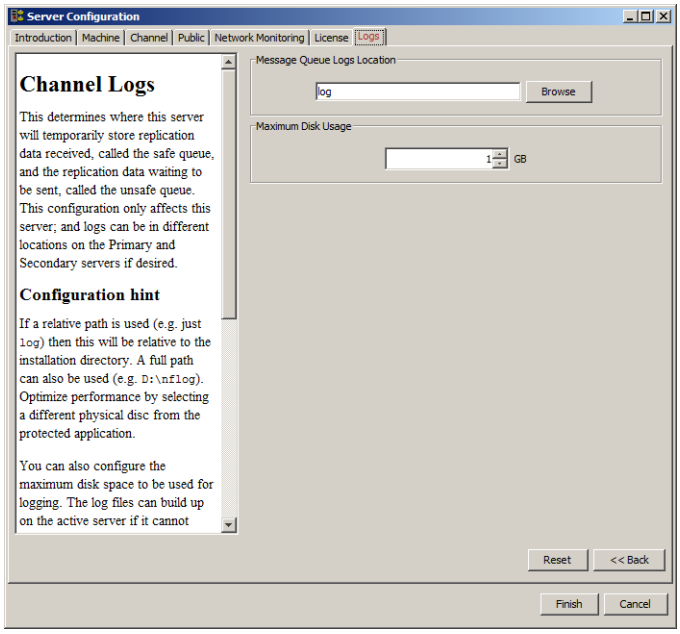
This configuration only affects the local server. Logs can be in different locations on the Primary and Secondary servers.

To configure the location of the message queue logs

1 Click the **Logs** tab.

2 Click **Browse** to navigate to the folder to store the message queue logs.

3 Select the folder and click **Next** or **Finish**.


Server Configuration
Introduction
Machine
Channel
Public
Network Monitoring
License
Logs
Channel Logs
This determines where this server will temporarily store replication data received, called the safe queue, and the replication data waiting to be sent, called the unsafe queue. This configuration only affects this server; and logs can be in different locations on the Primary and Secondary servers if desired.
Configuration hint
If a relative path is used (e.g. just log) then this will be relative to the installation directory. A full path can also be used (e.g. D:\nflog). Optimize performance by selecting a different physical disc from the protected application.
You can also configure the maximum disk space to be used for logging. The log files can build up on the active server if it cannot
Message Queue Logs Location
log
Browse
Maximum Disk Usage
1
GB
Reset
<< Back
Finish
Cancel

Configuring the Maximum Disk Usage

You can configure the maximum disk space allocated for logging. Log files increase in size on the active server under the following conditions:

- If the active server cannot communicate with the passive server
- Certain operations on the passive server
- If the server is under heavy load

When the disk reaches quota, replication stops and the system is no longer protected.

If using a dedicated disk for log files, consider disabling the quota. To do this, set the quota to zero. If vCenter Server Heartbeat runs out of physical disk space, it must be shut down before it can resume replication. Set the quota with sufficient overflow space so vCenter Server Heartbeat can stop replicating gracefully.

To configure Maximum Disk Usage, click the **Logs** tab, type the maximum dedicated disk space allocated for message queue log files, and click **Finish**.

System Administration and Management

Server Protection 6

This chapter includes the following topics:

- "Server Protection Overview" on page 123
- "Checking the Server Pair Status" on page 124
- "Configuring Heartbeat Settings" on page 125
- "Configuring vCenter Server Heartbeat Shutdown Options" on page 126
- "Configuring Split-Brain Avoidance" on page 129

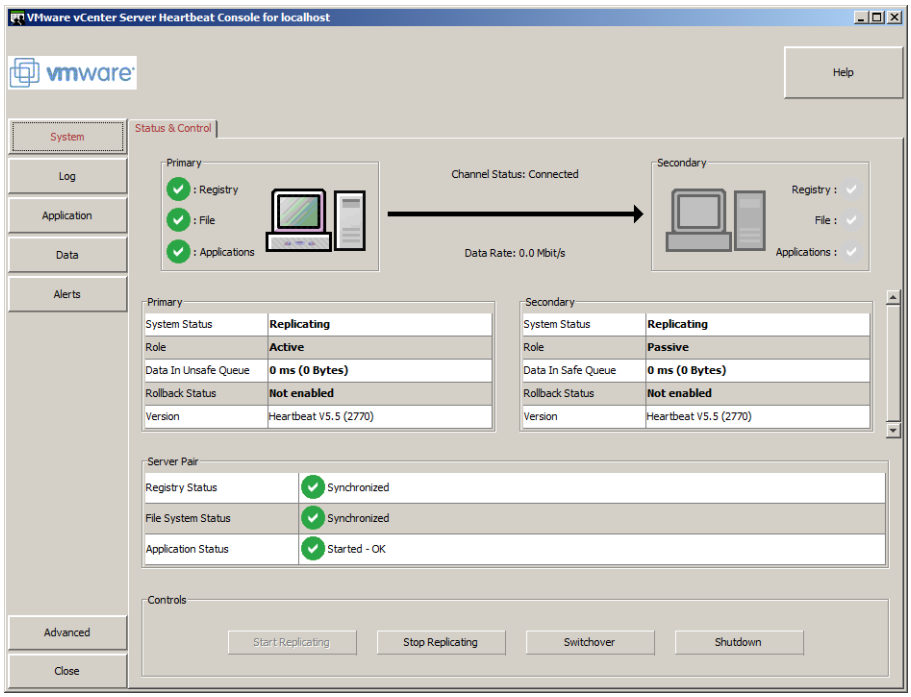
Server Protection Overview

Protection against failure of the operating system or hardware on the Primary server is facilitated by the two instances of the vCenter Server Heartbeat software monitoring each other by sending "I'm alive" messages and reciprocating with acknowledgments over a network connection termed the VMware Channel. If the passive server detects that this process or heartbeat fails, it initiates a failover.

vCenter Server Heartbeat proactively monitors the capability of the active server to communicate with the rest of the network by polling defined nodes around the network, including by default, the default gateway, the primary DNS server, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, due to network card failure or a local switch failure, vCenter Server Heartbeat can initiate a switchover, allowing the passive server to assume an identical network identity as the active server.

Checking the Server Pair Status

The **System** page is the first page that opens when administering a pair of servers. The **System** page displays the roles of the servers, active or passive, the actions that the servers are currently performing, and how well the system is coping with file and registry replication.



The system status in the central grid for each server indicates procedures being executed. Table 6-1 lists each status with a description.

Table 6-1. System Status

Status	Description
Not Replicating	The file and registry replication has stopped and all protected applications also could be stopped.
Stopping Replication	The file and registry replication is in the process of stopping and all protected applications also could be closing down.
Replicating	File and registry changes on the active server are being intercepted and replicated to the passive server and protected applications are being monitored (This is the normal status).
Starting Replication	The replication process is in the process of starting and protected applications are being started.
Shutting Down	The vCenter Server Heartbeat file and registry interceptor has stopped. All protected applications also could have stopped. The Neverfail Server R2 service is stopping.
Preparing to Switch	The system is performing ancillary operations prior to a switchover such as flushing the queues.
Switching	The system is in the process of performing a switchover.

The central grid also displays queue delays for each server. Queues show the time a specific piece of information resides in the passive server (safe) and active server (unsafe) queues respectively before moving to the passive server (safe) queue or committed to disk. Above the data grid, the connection status and speed are graphically represented. The **Server Pair** panel graphically displays the file and registry synchronization status with icons described in Table 6-2.

Table 6-2. File and Registry Status

Icon	Description
Synchronized	The files or registry are fully synchronized.
Unchecked	Files are present that are currently not checked. A full system check has not completed.
Synchronized and Busy Processing	The registry is currently in the process of being synchronized.
Checking	The differences in the registry are currently being checked to see if they are synchronized.
Out of Synch	The files or registry are not synchronized.

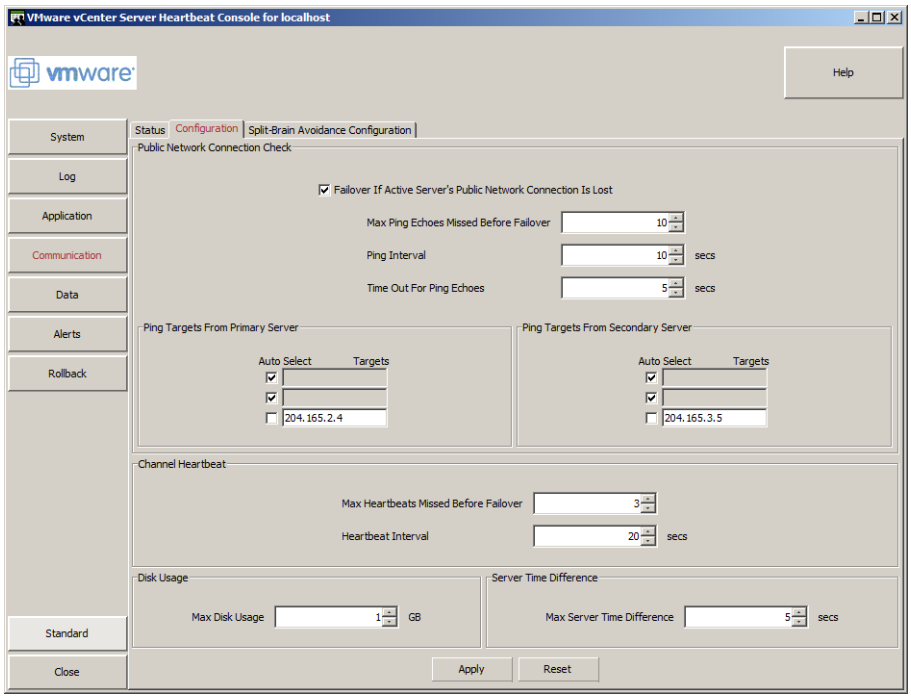
When the vCenter Server Heartbeat pair establishes a connection, it triggers a file synchronization and verification process to ensure all the files stipulated through file filters are mirror images of one another on their respective servers. The process checks each 64K block of all protected files and performs a checksum to find differences between blocks. When the checksum is the same, the block is marked as synchronized. When the blocks are different, the block is replicated to the passive server and then marked as synchronized. The file verification and synchronization process completes when all blocks of all files are marked as synchronized.

Configuring Heartbeat Settings

The Heartbeat interval dictates the time step at which the passive server sends Heartbeat packets to the active server across the VMware Channel connections. **Max Heartbeats Missed Before Failover** determines the number of missed packets before initiating a failover.

1 Click **Advanced** > **Communication** on the left navigation pane and click the **Configuration** tab.

2 Set **Max Heartbeats Missed Before Failover** and the **Heartbeat Interval** and click **Apply**.

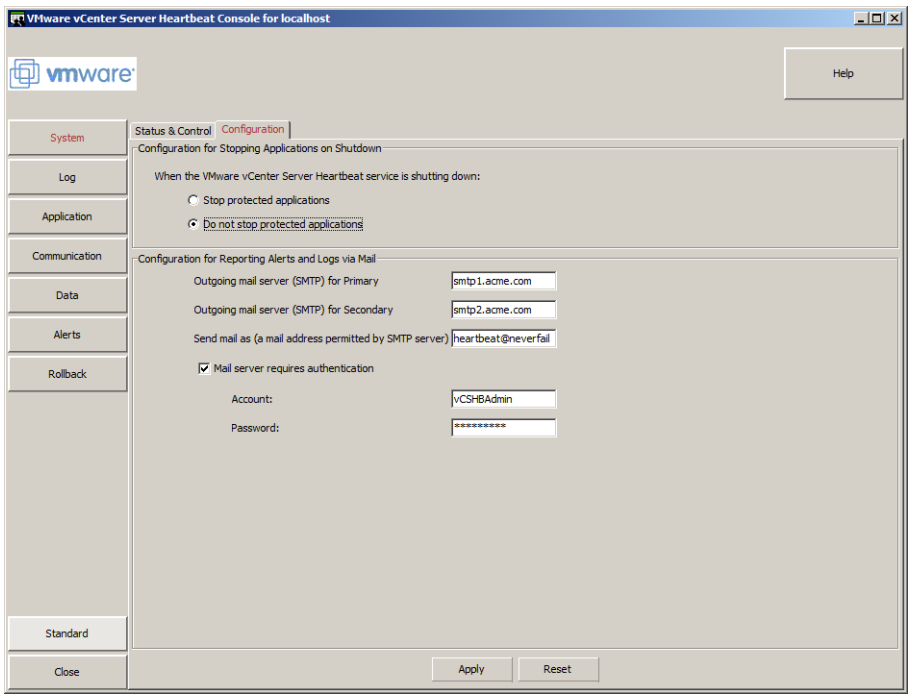


Configuring vCenter Server Heartbeat Shutdown Options

You can use vCenter Server Heartbeat to select whether to leave protected applications running upon shutdown or to stop protected applications as part of the shutdown process.

1 To set this option, click **Advanced** > **System** on the left navigation pane and click the **Configuration** tab.

2 Select the option vCenter Server Heartbeat performs when it shuts down. Click **Apply**.



Starting, Stopping, and Shutting Down vCenter Server Heartbeat

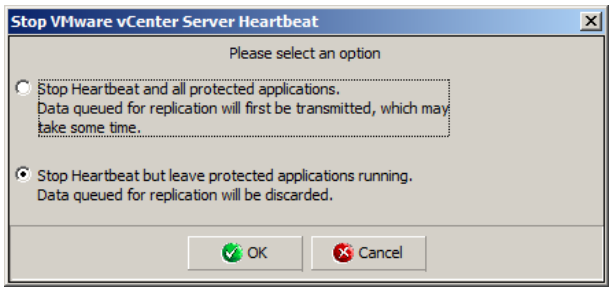
You can use **Start Replicating**, **Stop Replicating**, and **Shutdown** in the **System** page to configure the vCenter Server Heartbeat Server Service on both the servers synchronously.

Start Replicating

Start Replicating starts any application and data protection configured for the system. By default, all protection modes start when vCenter Server Heartbeat starts. Use **Start Replicating** only when the system has stopped activity with **Stop Replicating** or automatic stop.

Stop Replicating

Stop Replicating prompts you to stop parts of the system.


Stop VMware vCenter Server Heartbeat
Please select an option
Stop Heartbeat and all protected applications.
Data queued for replication will first be transmitted, which may take some time.
Stop Heartbeat but leave protected applications running.
Data queued for replication will be discarded.
OK
Cancel

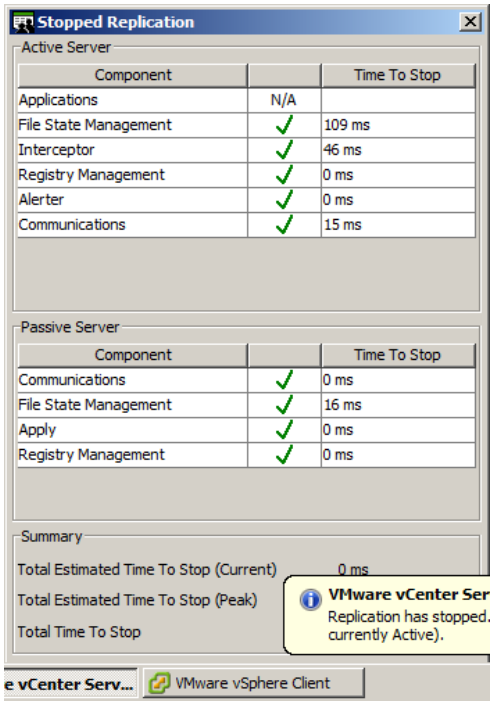
The default option, **Stop Heartbeat but leave protected applications running** stops the protection (synchronization) of data files but does not stop protected applications.

Stop Heartbeat and all protected applications stops the protection (synchronization) of data files and stops all protected applications.

The vCenter Server Heartbeat service continues to run on both the Primary and Secondary servers, providing heartbeats and continuing to protect the system and network facets of the active server.

For example, use **Stop Replicating** when a virus has infected the Primary server or when upgrading the protected application.

Click **OK** to view the stop status of the various facets of the server.



Shutdown

Shutdown is similar to **Stop Replicating** and stops all protection of data and when selected, protected applications. **Shutdown** also stops the vCenter Server Heartbeat Server service on both the active and passive machines. Use **Shutdown** when you must reconfigure the server or upgrade vCenter Server Heartbeat.

Forcing a Switchover

After configuring vCenter Server Heartbeat to protect all the required applications and data, the Secondary server can take over from the Primary server in a managed and seamless way called a switchover.

This is particularly useful during any maintenance work on the Primary server that involves restarting the server.

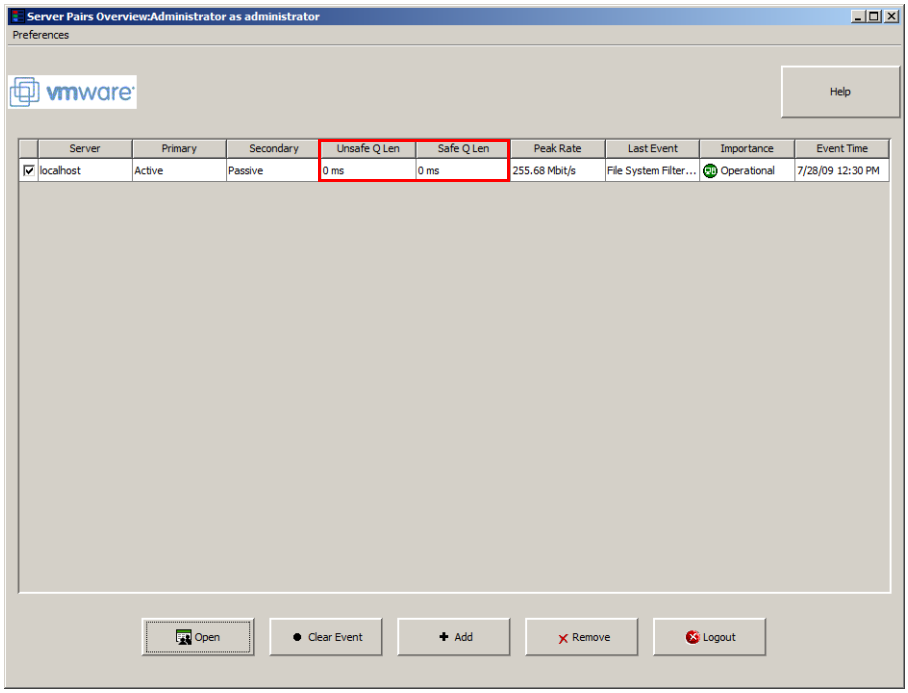
To initiate a switchover

Click **Switchover** in the **System** page to reverse the roles of the servers: the active server becomes passive and the passive becomes active. Users can continue to work without interruption while the Primary server is offline.

After the Primary server is again up and running, you can initiate the switchover again so that the Primary server becomes active and the Secondary server becomes passive.

NOTE You can perform a switchover whenever the systems are fully synchronized with respect to data files and registry replication. A switchover cannot occur if either server is in an unsynchronized or unknown state.

Before triggering a switchover, you should review the queue information. If the queues are large, file operations on the active server are very active. You must clear the queues before triggering a switchover. Review the queue lengths in the vCenter Server Heartbeat Console in the list of administered server pairs.



Recovering From a Failover

A failover differs from a switchover. A switchover is a controlled switch between the Primary and Secondary servers initiated manually from the vCenter Server Heartbeat Console, or initiated by vCenter Server Heartbeat when preconfigured conditions for switchover occur. A failover happens when one or all of the following have experienced a failure on the active server: power, hardware, or communications. The passive server counts a preconfigured number of missed Heartbeats before beginning a failover, and if this number is exceeded, assumes the active role and starts to execute the protected applications.

The following recovery scenario is based on vCenter Server Heartbeat configuration with the Primary server as active and the Secondary server as passive.

A failover has occurred and the Secondary server is now running as the active server.

1 Check event logs on both servers to determine the cause of the failover. For assistance, use the Log Collector tool to collect information and send the output to VMware Support.

2 Do not perform a switchback to the Primary server if the following issues occur on the Primary server. Resolve these issues before restarting vCenter Server Heartbeat:

- **Hard Disk Failure** – Replace the defective hard disk.
- **Power Failure** – Restore power to the Primary server.
- **Virus** – Clean the server of all viruses.
- **Communications** – Replace physical network hardware.
- **Blue Screen** – Determine cause and resolve. As required, submit the dump file to VMware Support (www.vmware.com/support) for analysis.

3 Run the Configure Server wizard and verify the server is set to Primary and passive.

4 Disconnect the VMware Channel network cables or disable the network card.

5 Resolve the list of possible failures.

6 Restart this server and reconnect or enable the network card again.

7 After restart, check that the **Taskbar** icon now reflects the changes by showing **P / –** (Primary and passive).

8 On the Secondary active server or from a remote client, launch vCenter Server Heartbeat Console and confirm that the Secondary server as active.

If the Secondary server is not displaying as active, perform the following steps:

1 If the vCenter Server Heartbeat Console is unable to connect remotely, try running it locally. If you are still unable to connect locally, use the Service Control Manager to verify that the service is running. If the service is not running, check the event logs for a cause.

2 Run the Configure Server wizard and check that the server is set to Secondary and active.

3 Verify that the protected application is accessible from clients. If so, start vCenter Server Heartbeat on the Secondary server. If the application is not accessible, check the application logs to determine why the application is not running.

4 Start vCenter Server Heartbeat on the Secondary active server.

NOTE The data on this server should be the most up to date and this server is the live server on the network. When vCenter Server Heartbeat starts, it overwrites all the protected data (configured in the File Filter list) on the Primary passive server. If you are not sure that the data on the active server is up to date, contact VMware Support (www.vmware.com/support). Go on to the next step only if you are sure that you want to overwrite the protected data on the passive server.

---

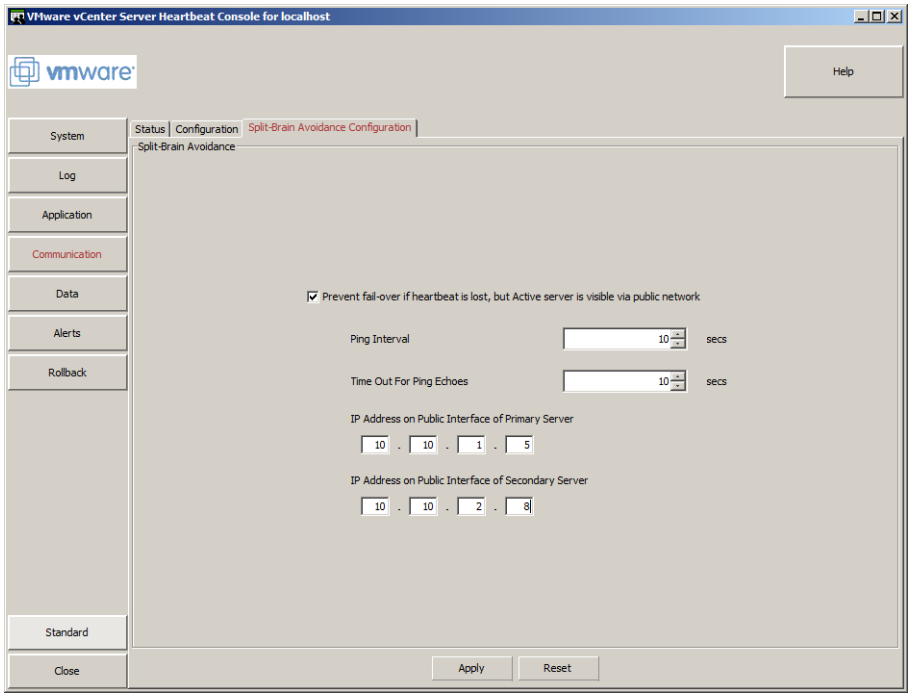
5 Start vCenter Server Heartbeat on the Secondary active server and check that the **Taskbar** icon now reflects the correct status by showing **S / A** (Secondary and active).

Configuring Split-Brain Avoidance

You can enable or disable the Split-brain Avoidance feature by selecting or clearing **Prevent fail-over if heartbeat is lost but Active Server is visible via public network**.

The passive server polls the active servers Principal (Public) connection at the time interval specified in the ping interval text box. You can increase or decrease the interval from the default 10 seconds as required.

The active server must respond within the time period value specified in the **Time Out for Ping Echoes** text box to prevent a failover. If the active server responds in a timely manner, the failover mechanism ceases. If the active server does not respond, the failover occurs.



Configure IP addresses for Split-brain Avoidance as required from those set at install time for both the Primary and Secondary servers.

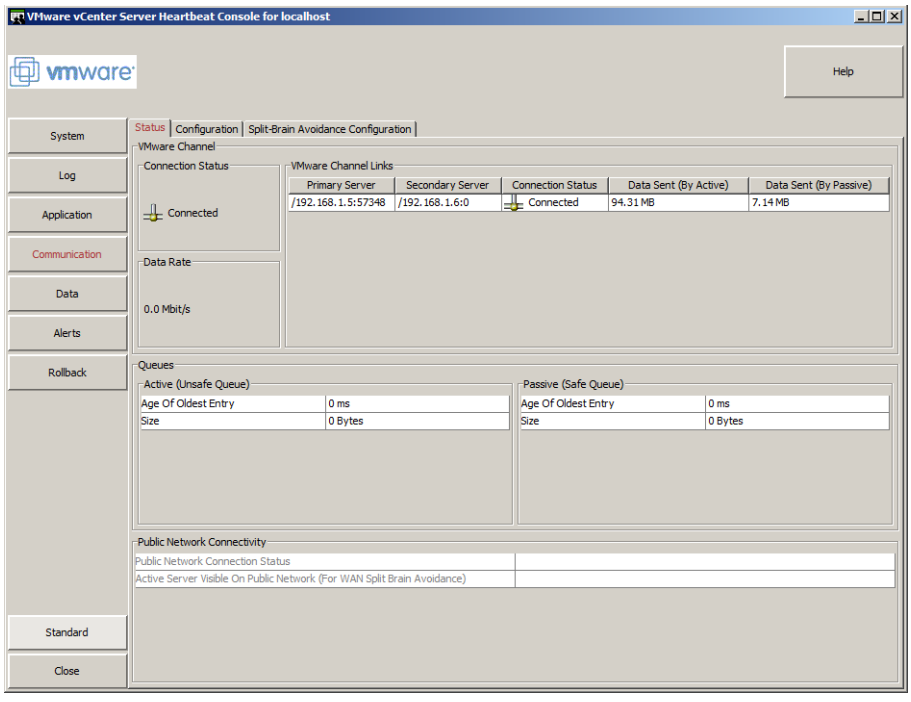
Network Protection 7

This chapter includes the following topics:

- "Communication Status" on page 131
- "Reviewing the VMware Channel Status" on page 131
- "Configuring Public Network Connection Checks" on page 132
- "Setting Max Server Time Difference" on page 133

Communication Status

Use the **Communication** page to check the status of the VMware Channel, the active server (unsafe) and passive server (safe) queues, and the Principal (Public) network.



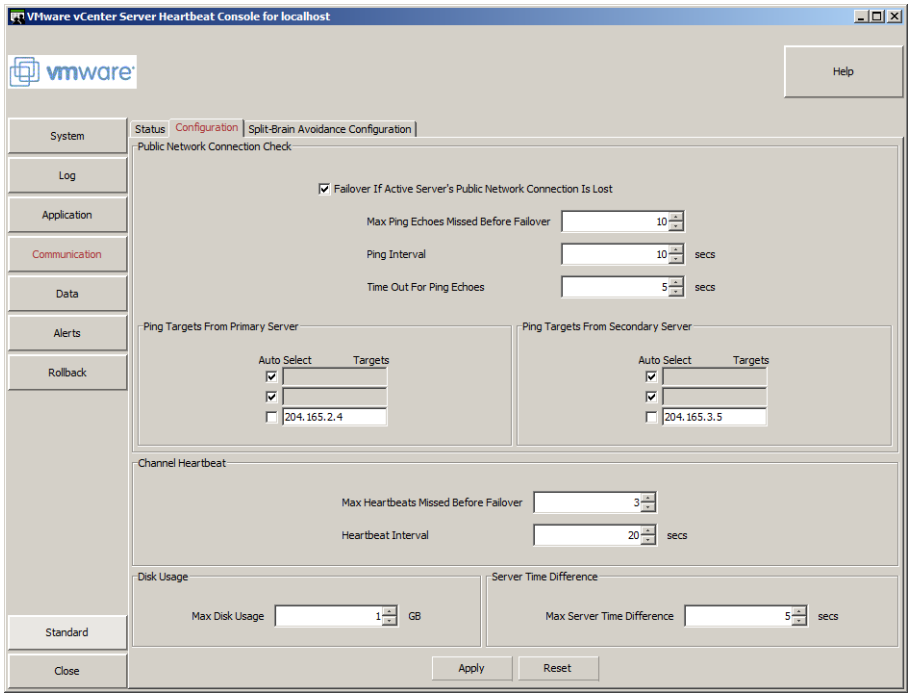
Reviewing the VMware Channel Status

The status displays connected or not connected, statistics of the connection about the data sent by either server, and the size and age of the oldest entry in the active server (unsafe) and passive server (safe) queues. The link status displays the IP address used by the VMware Channel for the Primary and Secondary servers with the port used for communications.

Public Network Connectivity displays the status of Principal (Public) network monitoring and or Split-brain Avoidance if configured on the server pair.

To configure VMware Channel communications, click **Advanced** and click the **Configuration** tab.

Configuring Public Network Connection Checks



Use the **Configuration** page to make adjustments to the Principal (Public) network monitoring features, the VMware Channel heartbeat features, the disk usage and server time difference.

Enable or disable Principal (Public) network monitoring by either selecting or clearing the **Failover if Active Server's Public Network Connection is Lost** check box. This feature integrates the polling of particular waypoints around the network through the Principal (Public) connection of the Active server to ensure connectivity with the Principal (Public) network. By default, it selects the IP addresses of the default gateway, the primary DNS server, and the Global Catalog server.

If one or more of the waypoints are co-located on a physical machine resulting in duplicate IP addresses, you can manually specify different waypoints. To specify a manual target for the Principal (Public) network checking, clear an **Auto Select** check box and manually overtype the IP address with the required target address.

In a WAN environment, the target addresses for Principal (Public) network monitoring on the Secondary server can be different from those selected on the Primary server. To override the discovered selections, clear the **Auto Select** check box and manually specify the target address.

Principal (Public) Network Monitoring operates when the active server effectively pings the target addresses at regular time intervals. The time interval is set by default to every 20 seconds but you can increase or decrease the frequency as required.

Each target has by default 5 seconds to respond. On slower networks where latency and network collisions are frequent, you can increase the response time. Adjust the **Timeout for Ping Echoes** value.

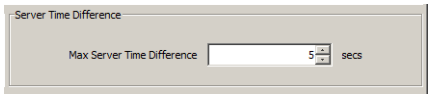
If any target fails to respond within the stipulated timeout, increase the polling interval to the timeout value until you receive a response. Then decrease the polling interval to the default time interval specified.

If all three targets fail to respond by missing the maximum pinged echoes and exceed the failover threshold value, vCenter Server Heartbeat initiates a switchover.

To save changes to the configuration of the communications, click **Apply**. To reset all configuration settings to the last save or default settings, click **Reset**.

Setting Max Server Time Difference

vCenter Server Heartbeat generates a warning if the Primary and Secondary server system clocks are not synchronized. To override the warning, allow the servers a maximum time difference specified in the **Max Server Time Difference**.



To save configuration of the communications, click **Apply**. To reset all configuration settings to the last save or default settings, click **Reset**.

Application Protection 8

This chapter includes the following topics:

- "Application Protection Overview" on page 135
- "Applications Tab" on page 135
- "Services Tab" on page 141
- "Tasks Tab" on page 146
- "Plugins Tab" on page 149

Application Protection Overview

vCenter Server Heartbeat incorporates an Application Management Framework (AMFx) to manage vCenter Server Heartbeat plug-ins.

The AMFx provides additional functions while maintaining the traditional stability of VMware software. Use the AMFx to install and remove plug-ins on the fly while vCenter Server Heartbeat continues to provide protection to currently installed applications.

The AMFx also employs sponsorship for protected application files and services. With sponsorship, multiple plug-ins can share files or services. When removing a plug-in, sponsorship prevents removal of a shared file or service that is still required by a remaining plug-in.

vCenter Server Heartbeat uses the **System** plug-in to monitor the server performance. With the **System** plug-in, you can configure a variety of counters and assign actions when associated rules are exceeded.

Applications Tab

The **Applications** page displays the status of protected applications and application health. From this page, you can start, stop, and configure all protected applications. You can view application events as they occur in the lower panel of the Application Log.

1 Log in to the vCenter Server Heartbeat Console.

2 Click **Application** on the left navigation pane and click the **Applications** tab.

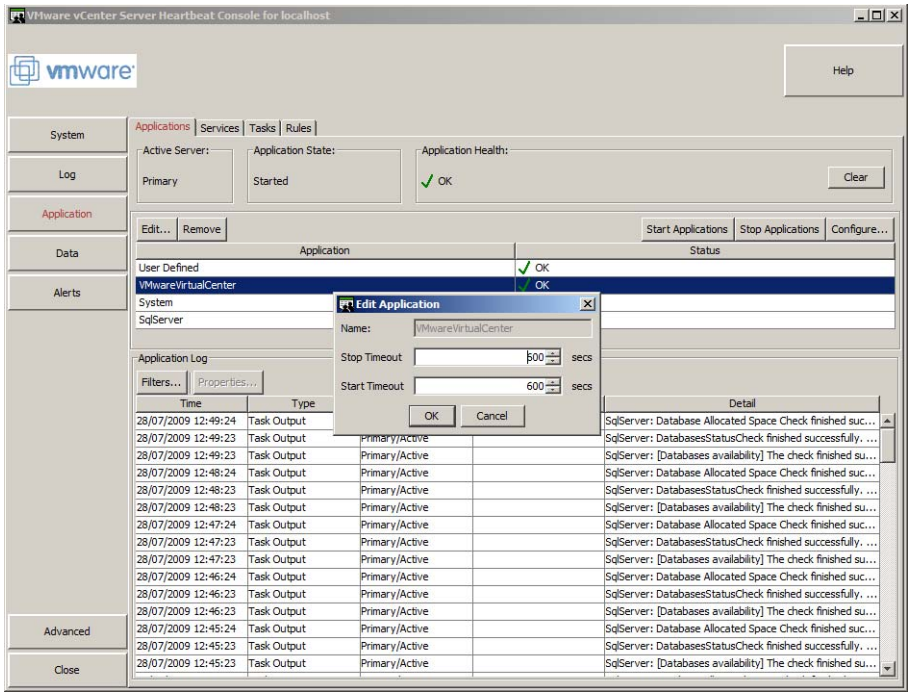
Editing Individual Applications

Use vCenter Server Heartbeat to configure the amount of time to wait for an application to start or stop before taking action or reporting the failure.

To configure the timeout settings

1 Select the application and click **Edit**.

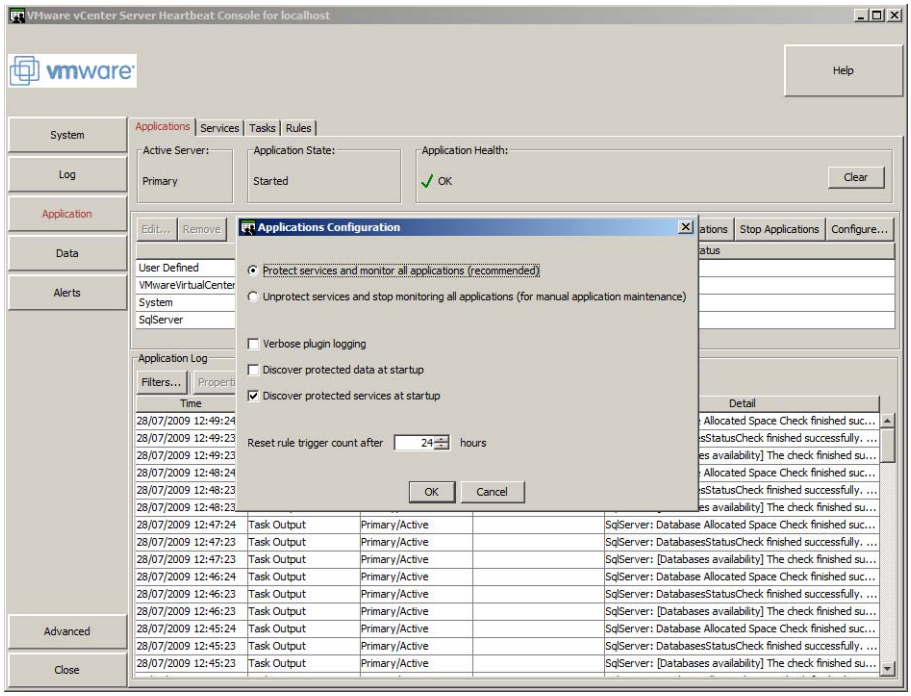
2 Type the settings, in seconds, for **Start Timeout** and **Stop Timeout** into the respective text boxes, and click **OK**.



Configuring Applications

Use the **Applications** page to configure protected applications, enables and disables protection and monitoring. You can maintain applications without stopping vCenter Server Heartbeat or taking the full server offline. During installation, vCenter Server Heartbeat sets default settings for application configurations but accepts modifications to the configurations settings.

1 Click **Configure** in the **Applications** page.

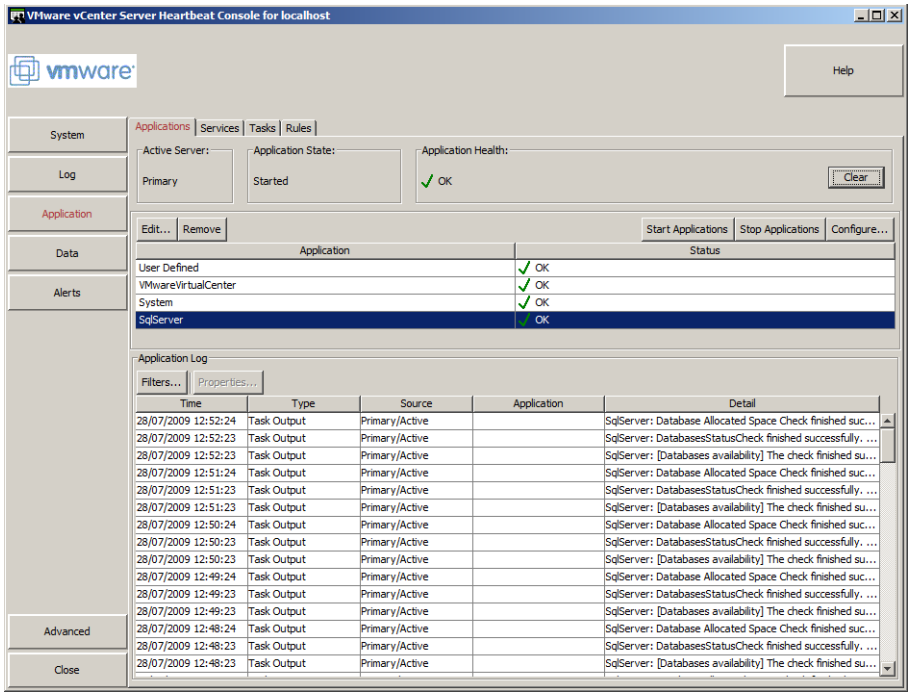


You can protect services and start monitoring applications or unprotect services and stop monitoring an application. You can also enable **Verbose Plugin logging**, **Discover protected data at startup**, **Discover protected services at startup**, and set the rule trigger count.

2 Click **OK**.

Reviewing the Status of an Application

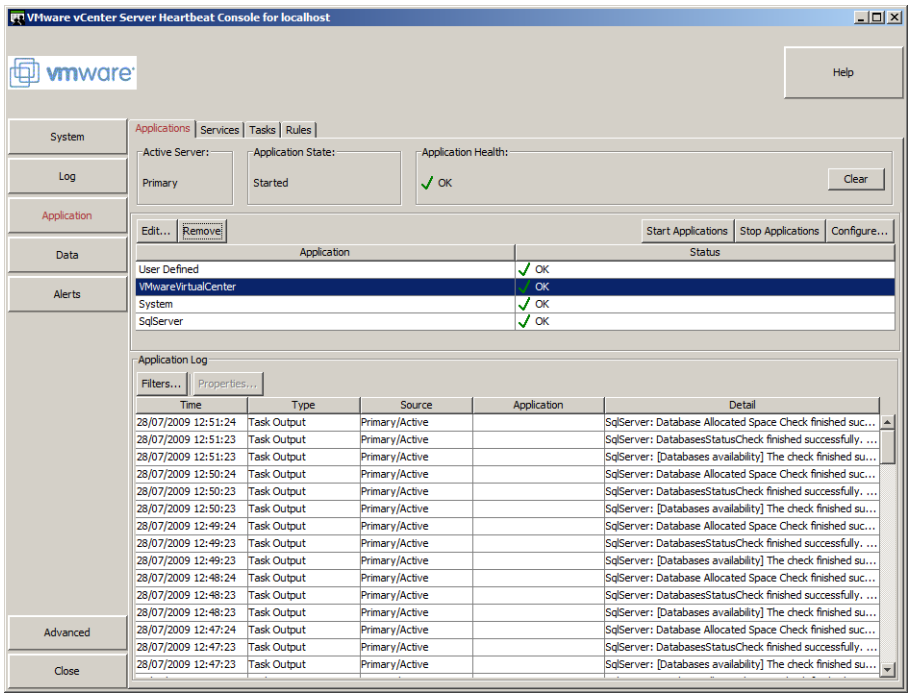
After an application successfully starts and is running, you can view the application status in the **Applications** tab of the **Application** page.



If an application fails, right-click the **Log** and investigate the failure.

Reviewing the Application Log

The **Application Log** helps troubleshoot the protected application environment.



The **Application Log** provides information about the behavior of all protected applications and includes events such as task status changes, rule triggering, task outputs, and application warnings. Use this log to troubleshoot application errors.

Filtering Application Log Entries

vCenter Server Heartbeat can filter Application Log files to limit the events to display. By default, all events display in the Application Log file.

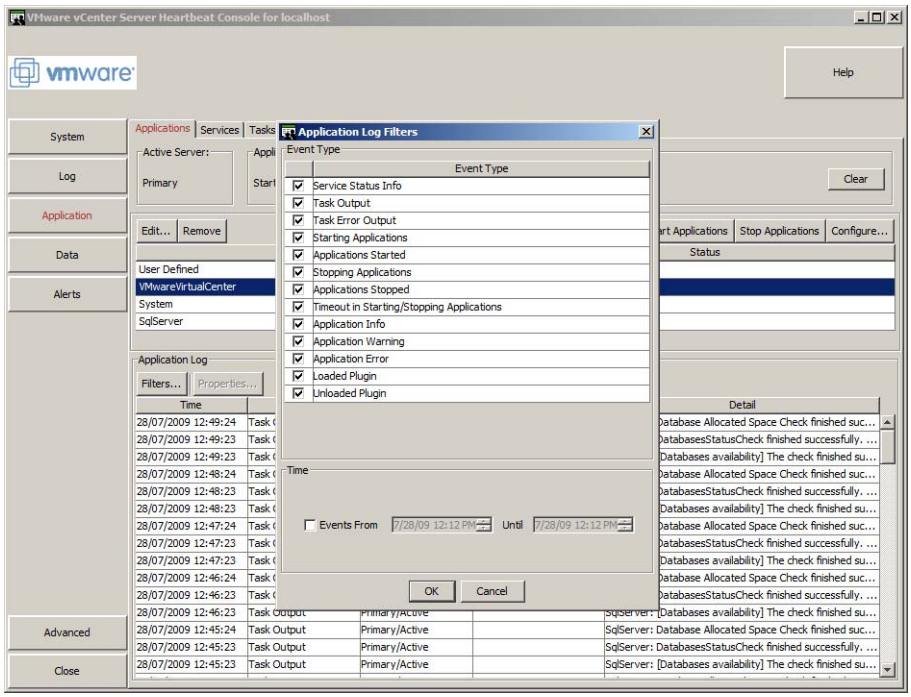
To filter the events to display

1 Click **Filter** in the **Application Log** panel on the **Applications** page.

2 In the upper section, clear the event types you do not want to view.

3 Configure a date and time range to limit the events to fit that date and time range. To limit the date and time range, select **Events From** and edit the date or time range.

4 Click **OK**.

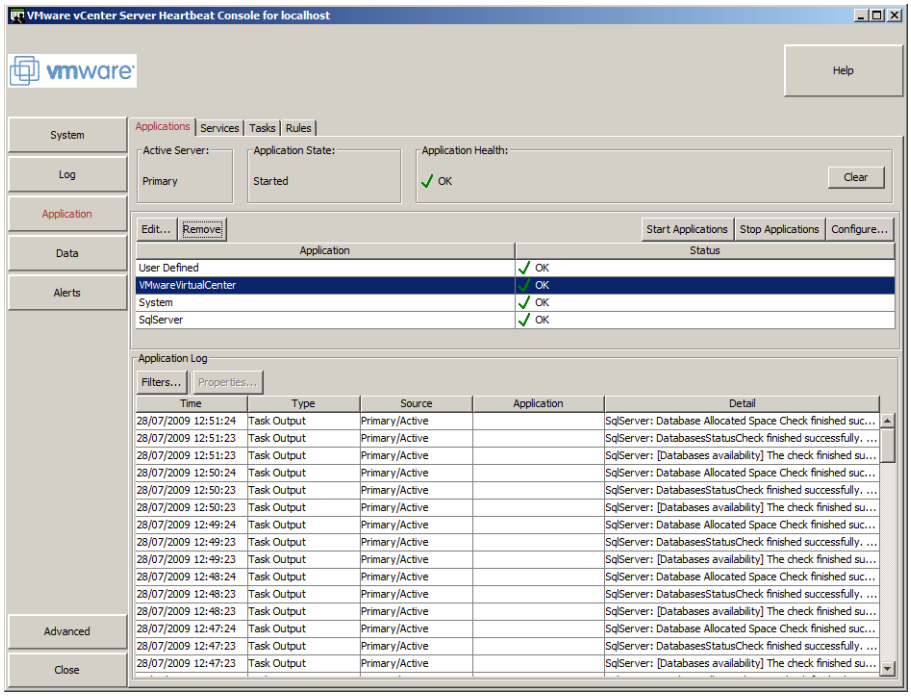


Resetting the Application Health Status

To reset the Application Health status

1 Click the **Applications** tab of the **Applications** page.

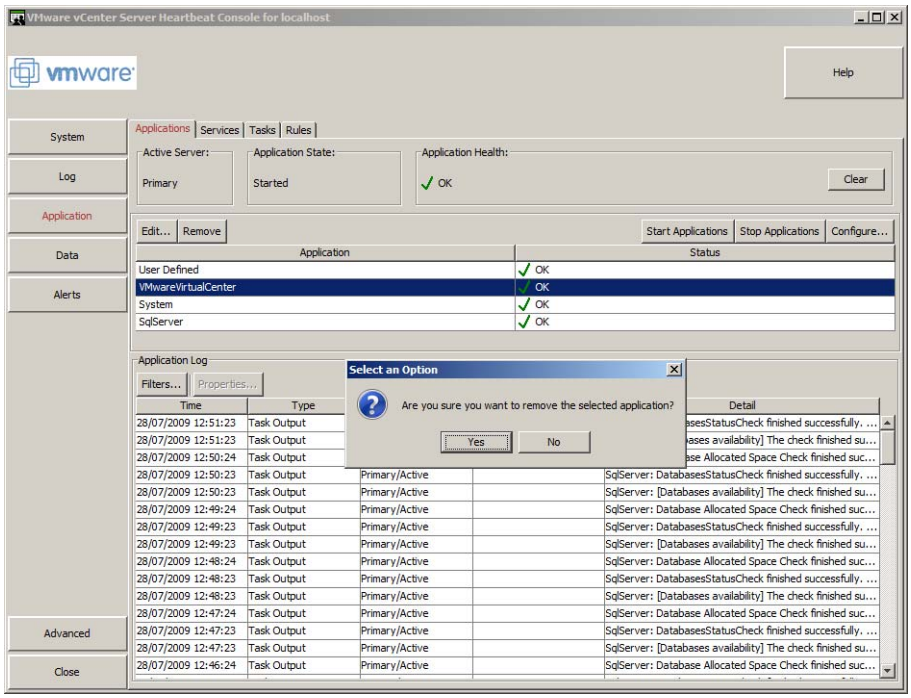
2 Click **Clear** in the Application Health panel.



Removing an Application

To remove an application, select it and click **Remove**.

If the sponsor of the selected application is associated with a plug-in, removing the application has the same effect as removing the plug-in. If the sponsor is not associated with a plug-in, all sponsorship is removed from services, filters, and tasks.



Services Tab

The **Services** page displays both services that you or plug-ins specify and the services related to them by dependency (either as dependents or depends-on). The target states of protected services for the active and passive server can be specified and are typically **Running** on the active and **Stopped** on the passive. Services are protected if they are **Running** or **Automatic**, and are otherwise logged as unprotected. vCenter Server Heartbeat manages services that depend on protected services (started and stopped) but not monitored (not restarted if stopped by some external agency). vCenter Server Heartbeat monitors protected services (restarted if stopped) but not managed (not stopped if protected applications are stopped).

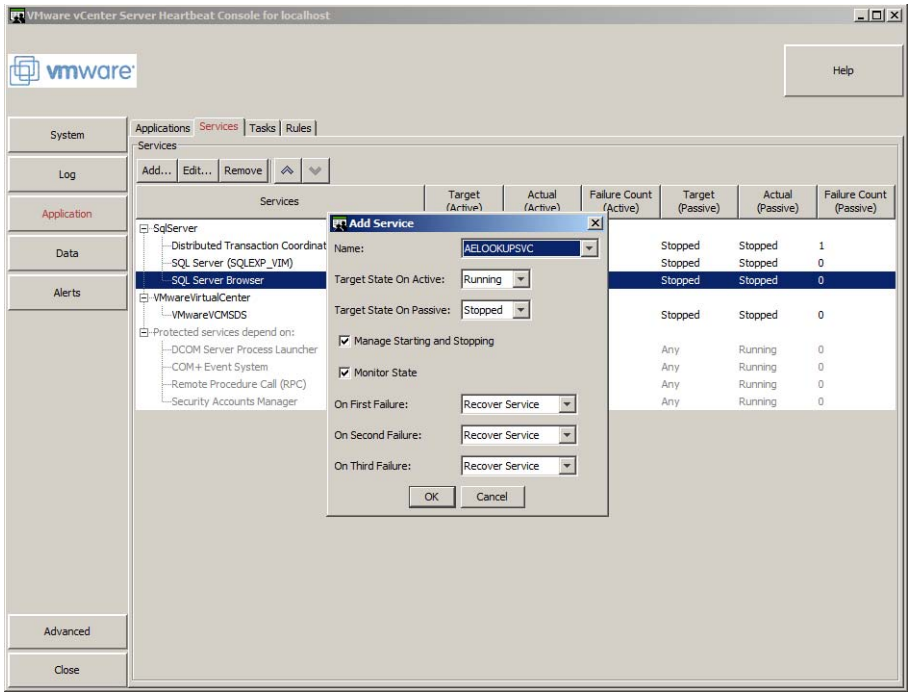
Log in to the vCenter Server Heartbeat Console, click **Application** on the left navigation pane and click the **Services** tab.

Adding a Service

To protect a service

1 Add the service from the vCenter Server Heartbeat Console in a Running state.

2 Click **Add** to see a list of running services under **Name**.



3 Select the service and set the values for **Target State on Active** and **Target State on Passive**. Normally the **Target State on Active** is set to **Running** and the **Target State on Passive** is set to **Stopped**.

NOTE Setting the target state for both the active and passive server to **Running** can cause the service to place a lock on some files preventing synchronization from completing.

4 If vCenter Server Heartbeat is to manage the start and stop of the service, select **Manage Starting and Stopping**. If vCenter Server Heartbeat is to monitor the state of the service, select **Monitor State**.

vCenter Server Heartbeat also assigns three sequential tasks to perform in the event of failure. Task options include **Recover Service**, **Application Restart**, **Log Warning**, and any additional user-defined tasks previously created.

NOTE For dependent services, failure actions must match the protected service.

5 Assign a task to each of the three failure options and click **OK**.

NOTE If an application with the failure option set to **Application Restart** fails, only the services that have failed are restarted. Dependent services do not stop and restart as a result of the failure.

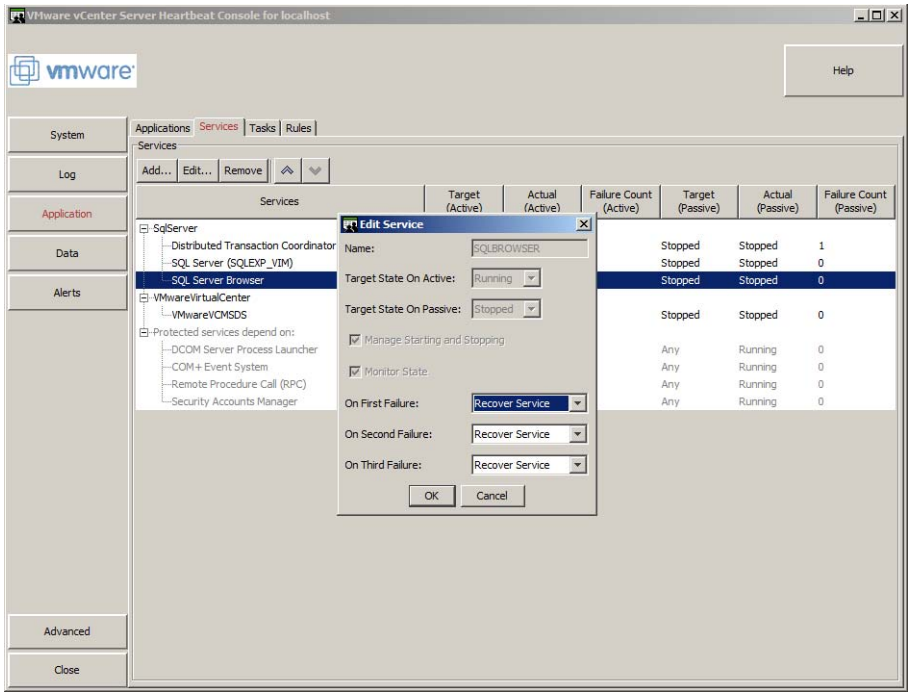
Editing a Service

To change the options of a protected service

1 Select the service and click **Edit...**

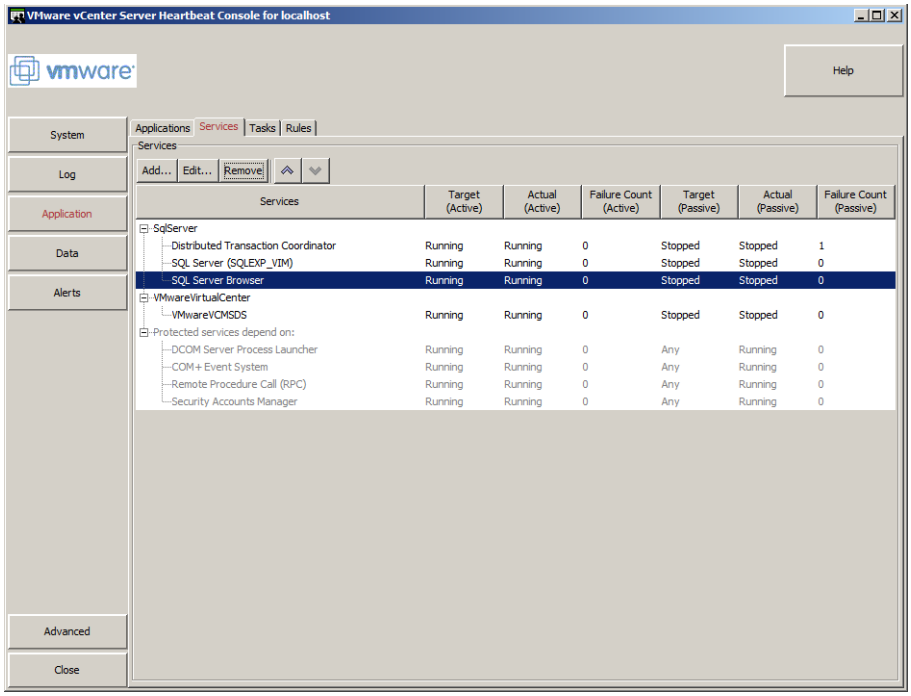
The Edit Service window opens to provide a subset of same options available when adding a new service.

2 Make the modifications and click **OK**.



Checking the Status of Services

The **Services** page displays the status of all protected services. The status shows both the target and actual state for both the Primary and Secondary servers and the Failure Counts for both servers.

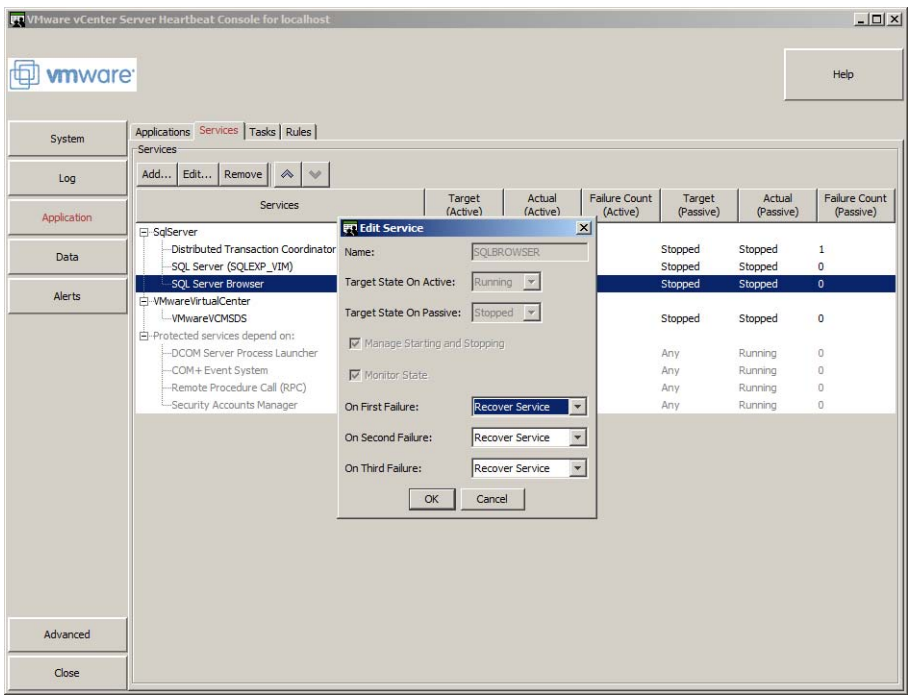


Unprotecting Services and Stopping Monitoring

To unprotect and stop monitoring the service

1 Click the **Services** tab. Select the service and click **Edit**.

2 Clear **Manage Starting and Stopping** and **Monitor State**. Click **OK**.



The order of services can be modified using **Up** and **Down** arrows. The exact order in which services start and stop is influenced by a number of key factors:

- The order of applications specified by plug-ins determines which services are started first.
- Services can have dependencies, and these must be respected. For example, if service B is listed after service A under the User-Defined group, and service A depends on Service B, Service B starts first.
- Multiple applications can use the same service (the same service can appear under more than one sponsor). The service starts when the first application to reference it starts.
- The order of stopping services is the reverse for starting services.

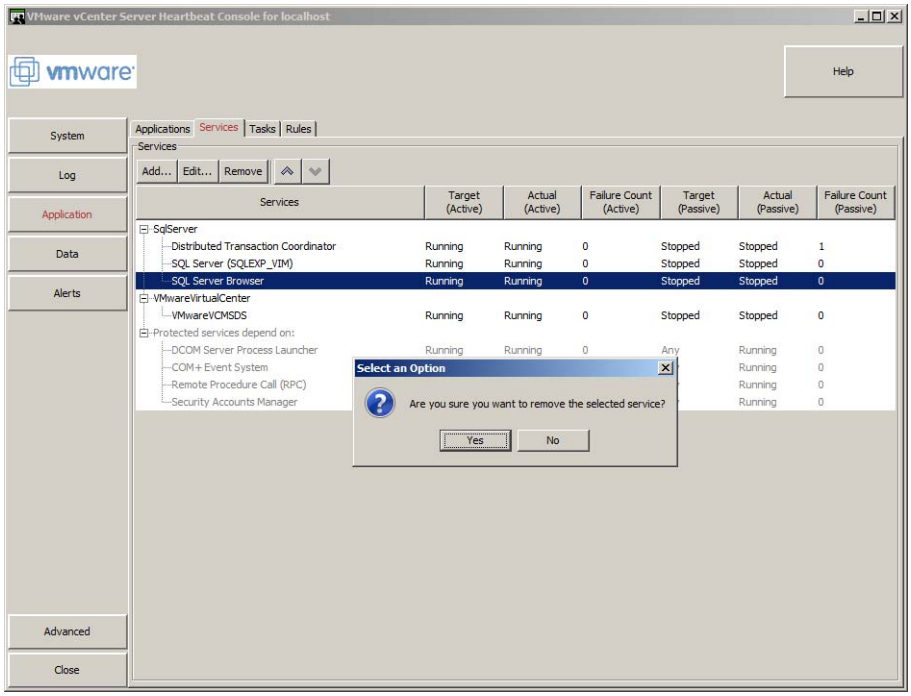
Removing a Service

To remove a service

1 Select the service.

2 Click **Remove**.

The service is removed from the protected list.



Tasks Tab

Tasks are a generalization and extension of the start, stop, and monitor scripts. Task types are determined by when the tasks run, and include the following:

- **Network Configuration** – This is the first type of task that runs when applications start and is intended to launch `dnscmd` or DNSUpdate. The task can launch a batch script containing multiple `dnscmd` commands. Network Configuration tasks are the only types of task that can vary between Primary and Secondary servers.
- **Pre/Post Start** – These tasks run before and after services start on the active server.
- **Pre/Post Stop** – These tasks run before and after services stop on the active server.
- **Pre/Post Shadow** – These tasks run before and after Data Rollback Module creates a shadow copy on the active server.
- **Rule Action** – Configure these tasks to run in response to a triggered rule or when a service fails its check.

You can define and implement tasks at the command line, such as launching a batch-script. Examples of built-in tasks include monitoring a protected service state on the active and passive servers.

vCenter Server Heartbeat can use plug-ins to define and implement tasks. An example of a plug-in-defined task is the discovery of protected data and services for a particular application.

Click **Application** on the left navigation pane, and click the **Tasks** tab.

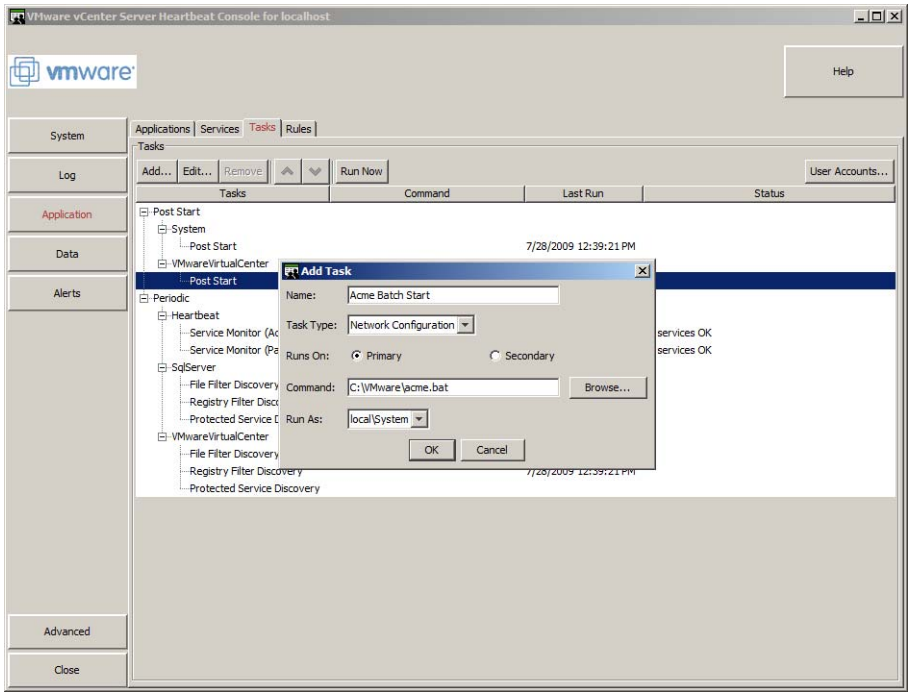
Adding a Task

To add a task

1 Click **Add**. Assign a name to the task and select the task type from the list.

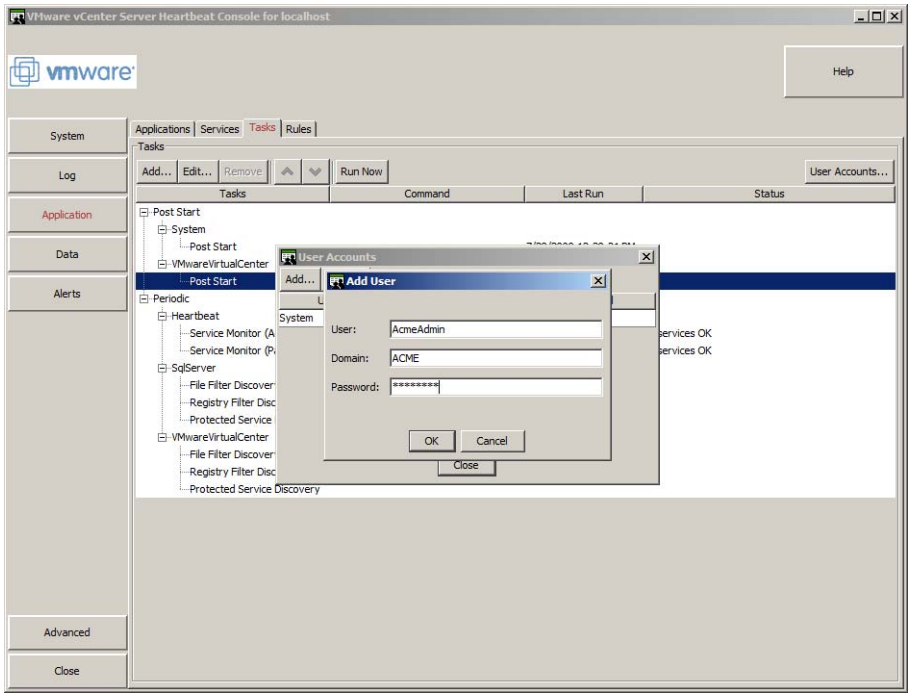
2 Add the appropriate information for the task type.

3 Click **OK**.



4 If the **Command** requires specific user credentials, click **User Accounts...** in the upper right of the page.

5 Add user accounts to make them available as a selection in **Run As** when you add a task.

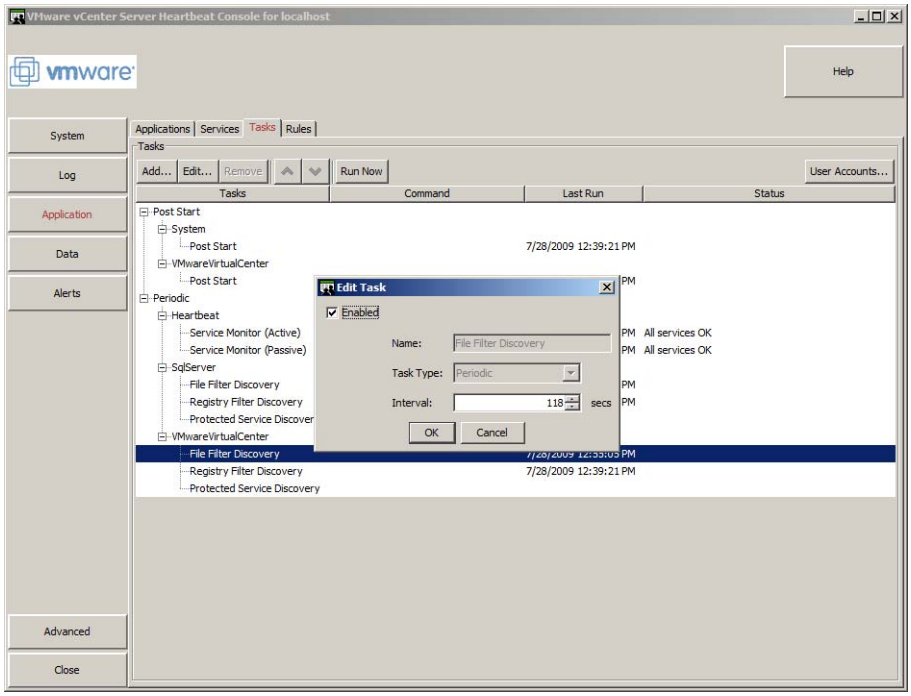


Editing a Task

To edit a task

1 Select the task and click **Edit**. You can edit the task interval or disable the task.

2 Click **OK**.

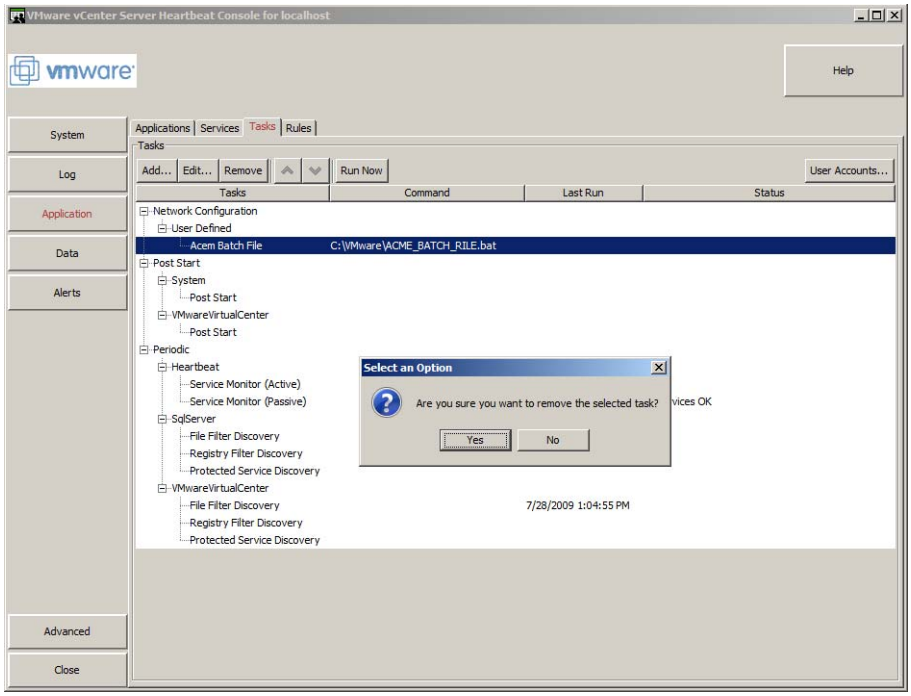


Removing a Task

To remove a task

1 Select the task.

2 Click **Remove**.



Starting a Task Manually

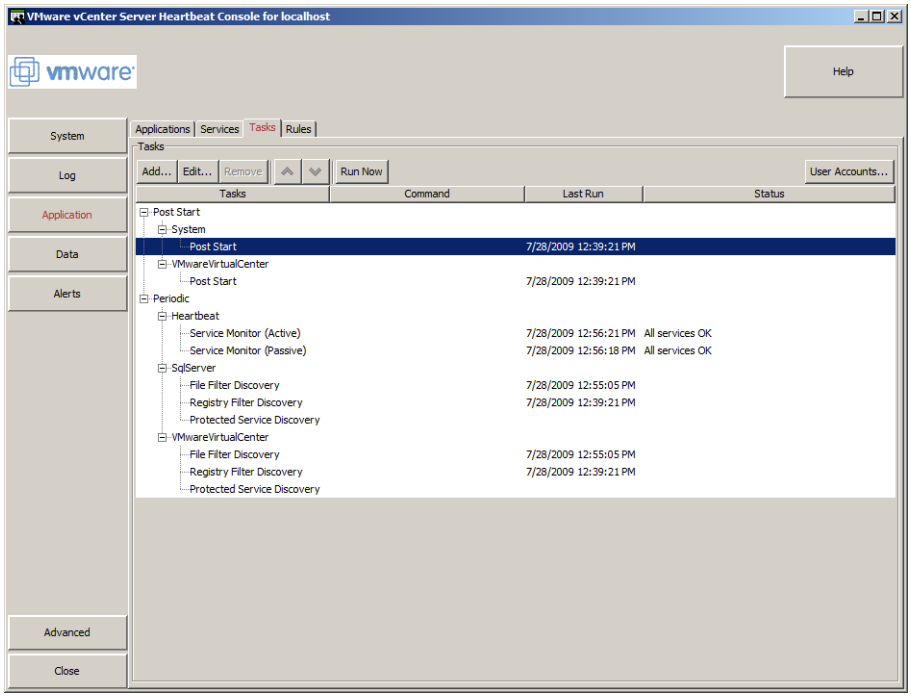
vCenter Server Heartbeat provides options to launch a task immediately, or to launch a task after a designated time period elapses, or following the occurrence of a specified event.

To launch the task immediately

1 Select the task.

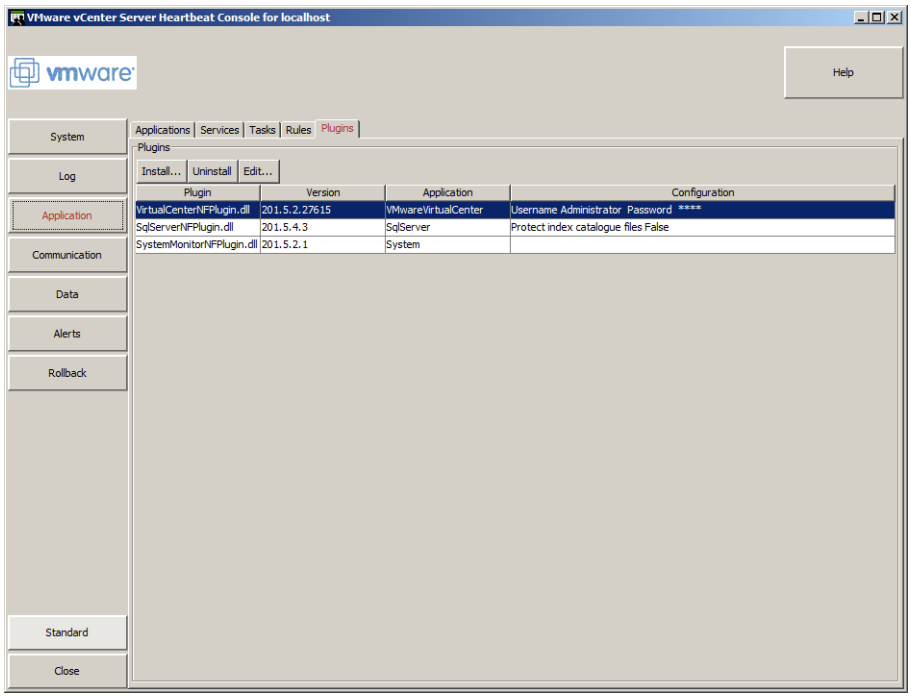
2 Click **Run Now**.

vCenter Server Heartbeat immediately launches the task.



Plugins Tab

Plug-ins support specific applications and contain all of the components to protect the designated application. Plug-ins start and stop the application, monitor the application, and provide all rules necessary to ensure that application is available in the event of a failure by initiating a configured auto-switchover.



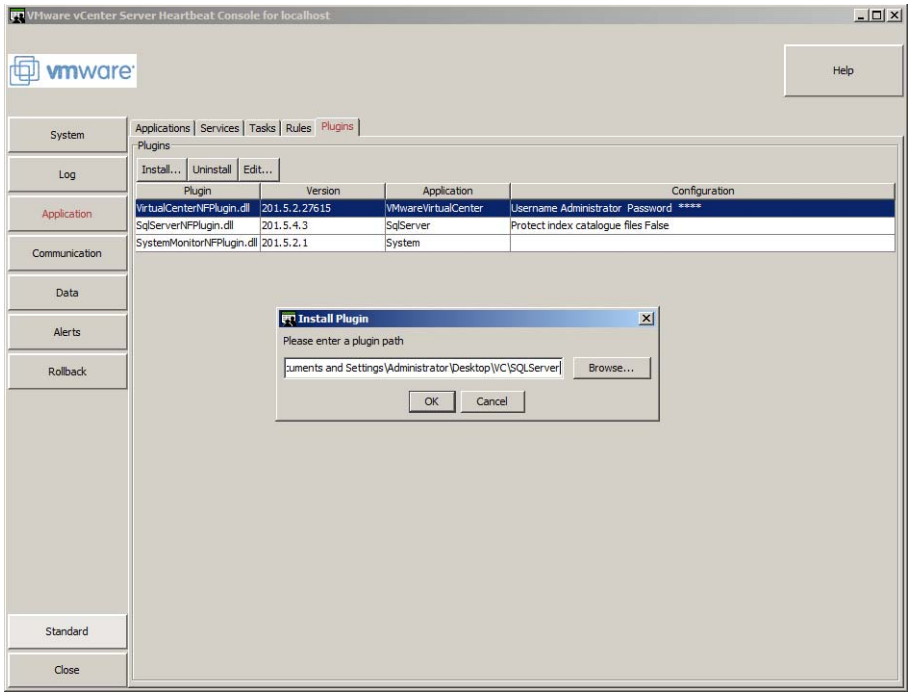
Installing a Plug-In

To install a new plug-in

1 Click **Application** and click the **Plugins** tab.

2 Click **Install...** and browse to the plug-in. The path statement is case-sensitive.

3 Click **OK**.



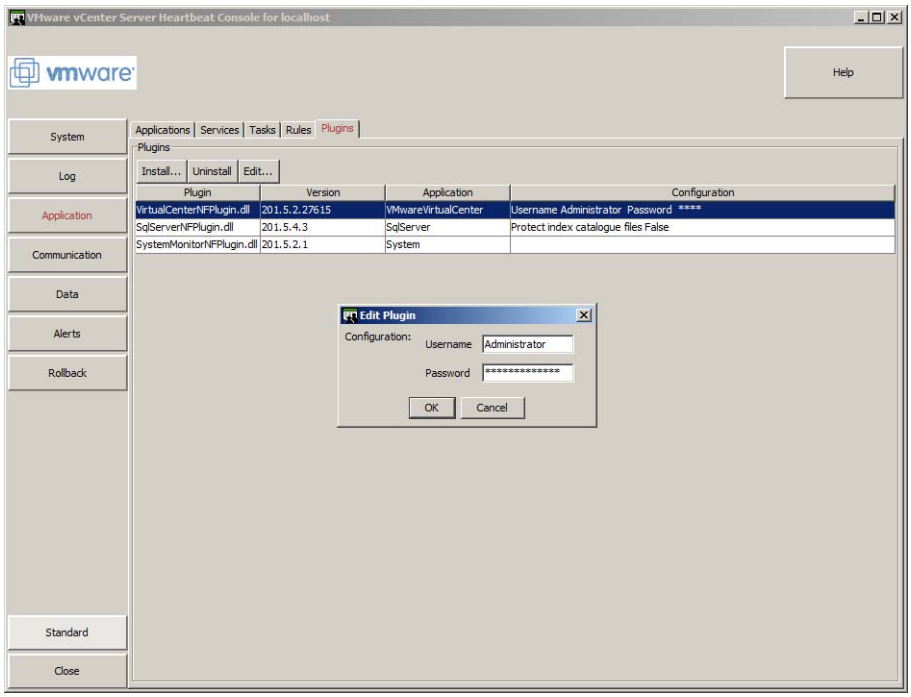
Editing a Plug-in

To edit the plug-in configuration

1 Select the plug-in and click **Edit** to modify the default configuration.

2 Review the configuration options before making modifications as they are specific to each plug-in.

3 Click **OK**.



Uninstalling a Plug-in

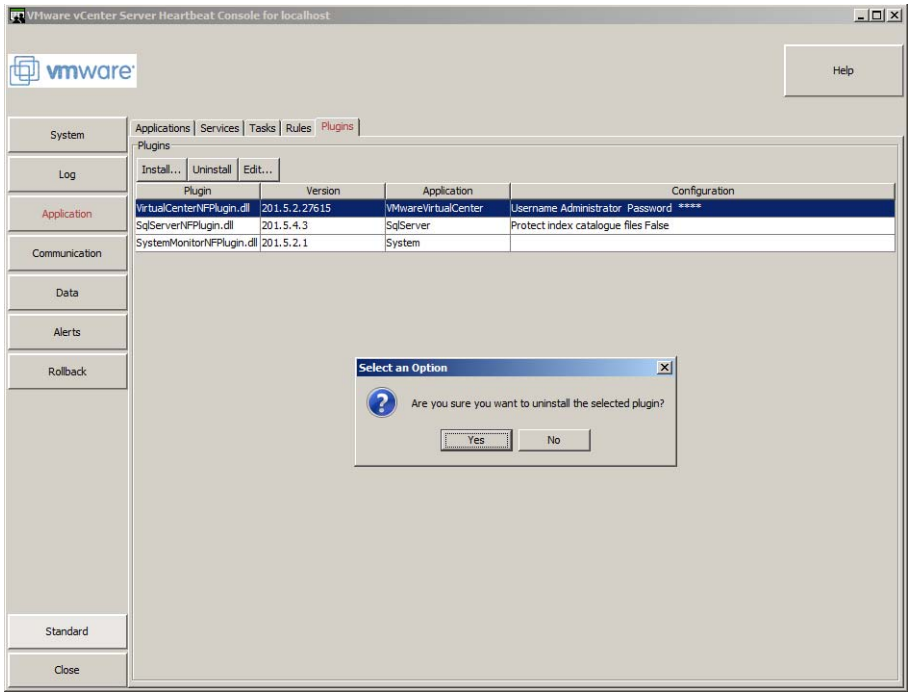
You can uninstall a plug-in when you upgrade or remove the application the plug-in protects, or when directed by VMware Support.

To uninstall a plug-in

1 Select the plug-in.

1 Click **Uninstall**.

The plug-in is uninstalled and removed.



Status and Control

9

This chapter includes the following topics:

- "vCenter Server Heartbeat Console" on page 153
- "Logging into vCenter Server Heartbeat" on page 153
- "Configuring the Look and Feel of the vCenter Server Heartbeat Console" on page 156
- "Logging Out of the vCenter Server Heartbeat Console" on page 157

vCenter Server Heartbeat Console

vCenter Server Heartbeat operates over a pair of vCenter Server Heartbeat servers and is administered in these pairs.

The vCenter Server Heartbeat Console is used to carry out the day-to-day administration of one or more pairs of servers.

The vCenter Server Heartbeat Console runs from either of the two servers in the pair or remotely from another machine in the same subnet that has vCenter Server Heartbeat or the vCenter Server Heartbeat Client Tools installed.

NOTE You can install vCenter Server Heartbeat on a Windows XP and Windows Vista SP1 or later workstation to act as a client to the server pair or Windows Server 2003. Run `setup.exe` from the `setup CD` folder on the workstation and select **Install Client Tools** under the installation set.

Logging into vCenter Server Heartbeat

To access vCenter Server Heartbeat, launch the vCenter Server Heartbeat Console from the desktop shortcut or **Start** > **All Programs** > **VMware** > **VMware vCenter Server Heartbeat** > **Manage Server**.

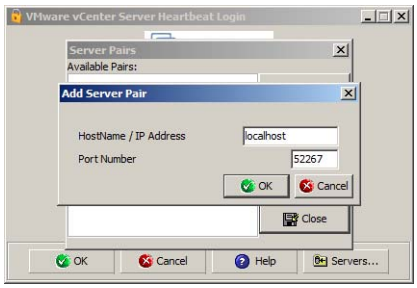
Before you log in, you must identify the pair of servers to administer. Click **Servers**.

NOTE It is recommended that you add the Principal (Public) IP address or the Fully Qualified Domain Name of the Primary server to ensure that you can administer the pair from the Heartbeat Console regardless of whether the current server is active or passive.

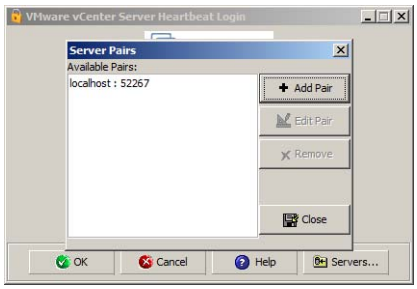
To add or remove a pair of vCenter Server Heartbeat servers

1 A **Server Pairs** window displays no servers in the **Available Pairs** list. To add a server pair, click **Add Pair**. The **Add Server Pair** window opens.

2 Type the IP address of the Primary server of any NIC on the active server or the NetBIOS name of the server pair and click **OK**.



3 The server pair appears in the list of **Available Pairs**. As required, sequentially add more server pairs to the list by repeating the procedure.



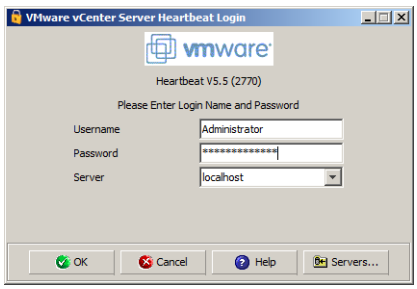
4 To edit a server pair, select it in the list and click **Edit Pair**. To remove a server pair, select it in the list and click **Remove**.

5 When finished, click **Close** to return to the login window.

Connecting to a Pair of Servers

To administer a pair of servers you must connect to them through the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes. Wait 10 seconds after starting vCenter Server Heartbeat before attempting to connect.

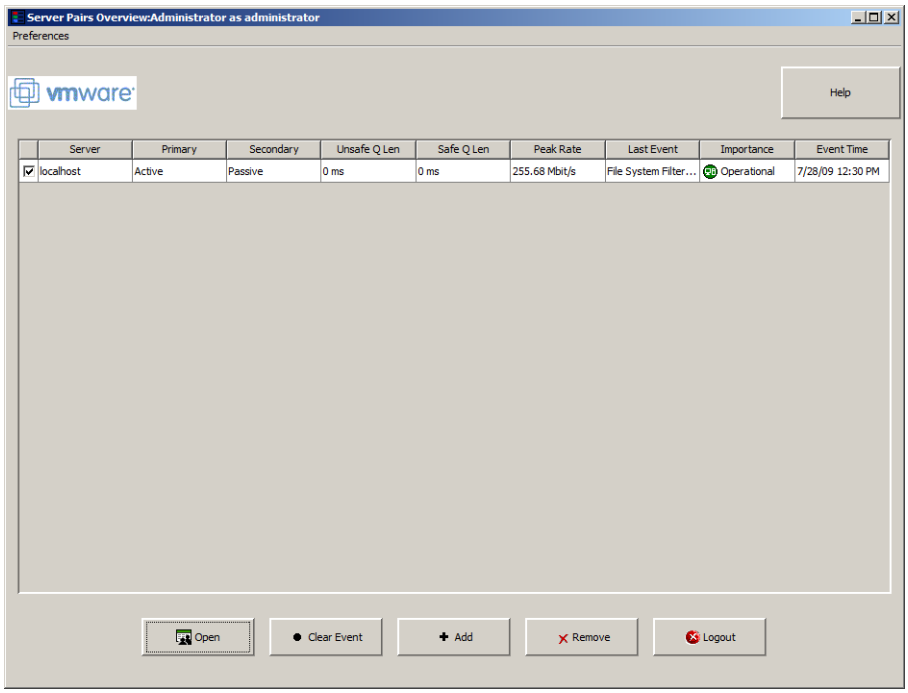
1 Select a server pair from the **Server** drop-down menu.



2 Type a **Username** and **Password** with valid Windows credentials into the respective text boxes. In a domain environment, use the format **`domainname\username`**.

Reviewing the Status of a Server Pair

The **Server Pairs Overview** window lists the selected pair of servers with other server pairs that historically were administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.

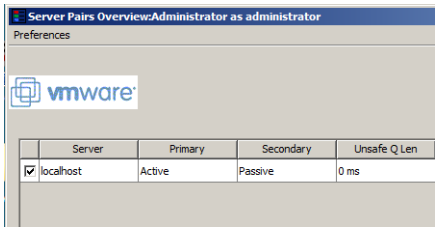


Additional information about the communications between the servers is displayed: the length of the passive server (safe) and active server (unsafe) queues and the peak rate of data transfer over the VMware Channel. **Last Event**, **Importance**, and **Event Time** also display. These events are discussed later in this guide.

To add additional pairs of servers

1 Click **Add** and follow the previously described procedure. **Exit** closes the interface but does not affect the vCenter Server Heartbeat Server service.

2 To select a pair listed in the main data grid, select the check box next to the server name.



When a pair is selected, the **Open**, **Clear Event**, and **Remove** buttons become active.

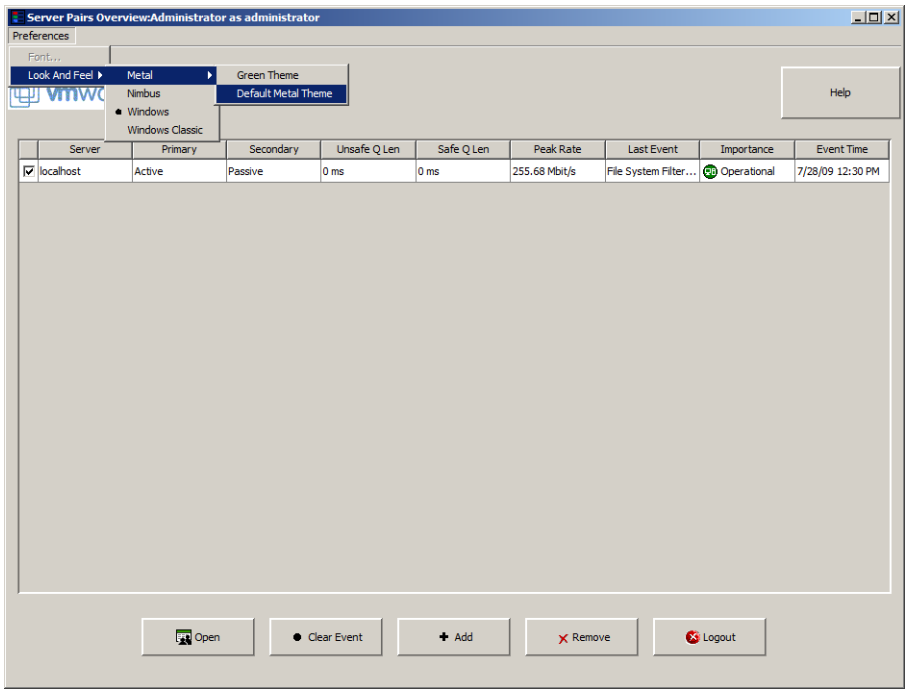
- **Clear Event** removes all events logged for that pair of servers and resets the log files for the pair of servers.
- **Remove** deletes the pair of servers from the vCenter Server Heartbeat Console.
- **Open** permits administration and configuration of the pair of servers.

Configuring the Look and Feel of the vCenter Server Heartbeat Console

Use the vCenter Server Heartbeat Console graphical user interface to change the style and color of the interface to suit your preferences.

To change the style of the interface

1 Launch the vCenter Server Heartbeat Console from the desktop shortcut or **Start** > **All Programs** > **VMware** > **VMware vCenter Server Heartbeat** > **Manage Server**.



2 In the **Server Pairs Overview** window, click **Preferences** and navigate to **Look and Feel**. Select a style to change the color and style of the interface.

Changing vCenter Server Heartbeat Console Pages

The buttons on the left of the window provide navigation between the pages of the vCenter Server Heartbeat Console.

You can determine the currently active page from the color of the text on the navigation buttons. The text on the active selection appears a magenta color, and inactive selections appear black.

Click **Log** to view the event log page.

Logging Out of the vCenter Server Heartbeat Console

To log out of the vCenter Server Heartbeat Console

1 Click **Close** to log out of administering the current server pair.

A confirmation window asks for confirmation of the logout request.

2 Click **Yes** to close the client and return to the **Server Pairs Overview** window.

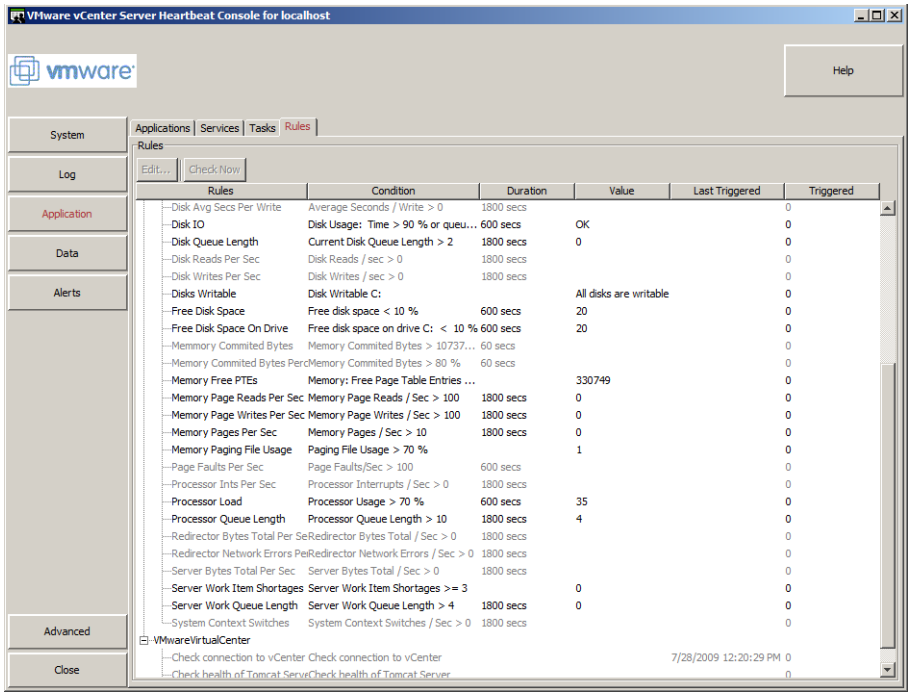
Performance Protection 10

This chapter covers the topic "Rules Tab" on page 159.

Rules Tab

Rules are implemented by plug-ins. There are no user-defined rules. Configure rule actions to trigger the rule that performs specific tasks. Rules have two trigger properties:

- **Timed** – They must evaluate as true continuously for the specified duration to trigger.
- **Latched** – They trigger as soon as they evaluate to true.



Editing a Rule

Each plug-in contains a default set of rules with options you can modify.

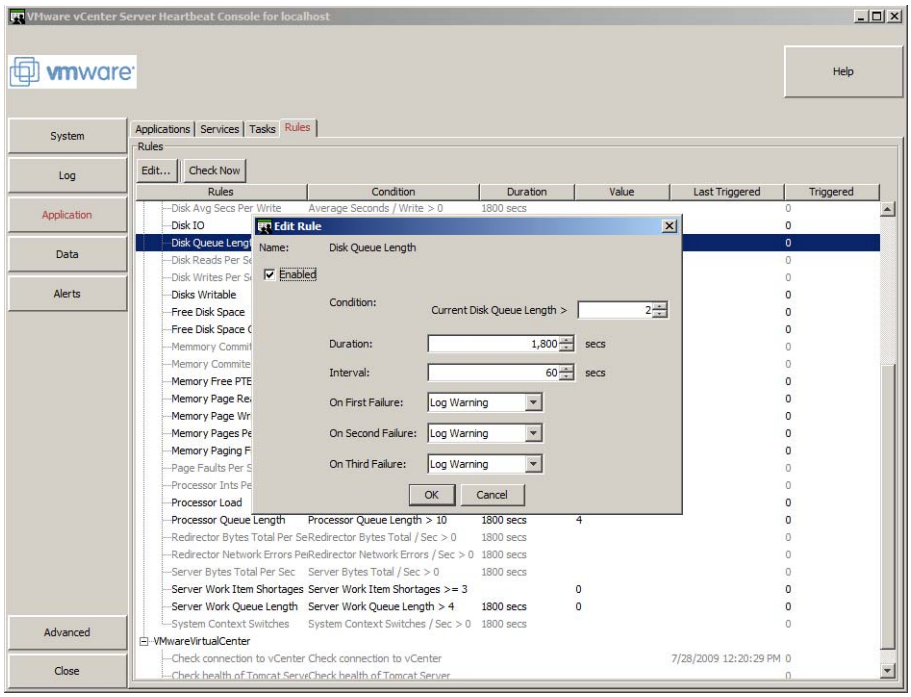
To edit a rule

1 Click **Application** in the navigation panel and click the **Rules** tab.

2 Select the rule and click **Edit**.

You can enable or disable a rule, set specific options, and assign tasks to be performed in the event of a first, second or third failure.

3 Click **OK**.



Rules Installed by vCenter Server Heartbeat Plug-Ins

The following plug-ins implement the rules listed.

vCenter Server Plug-In

- Check health of Tomcat server
- Check vCenter License
- Check Connection to vCenter

vCenter SQL Server Plug-In

- Default Instance Buffer Cache Hit Ratio
- Default Free Pages
- Default Instance Free Pages
- Named Instance Working Set
- Named Instance Buffer Cache Hit Ratio
- Named Instance Free Pages
- Named Instance Total Server Memory

vCenter Server Heartbeat System Plug-In

- DiskAvgSecsPerRead
- DiskAvgSecsPerWrite
- DiskIO
- DiskQueueLength
- DiskReadsPerSec
- DiskWritesPerSec
- DiskWriteable
- FreeDiskSpace
- FreeDiskSpaceOnDrive
- MemoryCommittedBytes
- MemoryCommittedBytesPercent
- MemoryFreePTEs
- MemoryPageReadsPerSec
- MemoryPageWritesPerSec
- MemoryPagesPerSec
- MemoryPagingFileUseage
- PageFaultsPerSec
- ProcessorIntsPerSec
- ProcessorLoad
- ProcessorQueueLength
- RedirectorBytesTotalPerSec
- RedirectorNetworkErrorsPerSec
- ServerBytesTotalPerSec
- ServerWorkItemShortages >= 3 (if the rule for server work item shortages is triggered, consult Microsoft documentation on setting the registry values for InitWorkItems or MaxWorkItems accordingly).
- ServerWorkQueueLength
- SystemContextSwitches

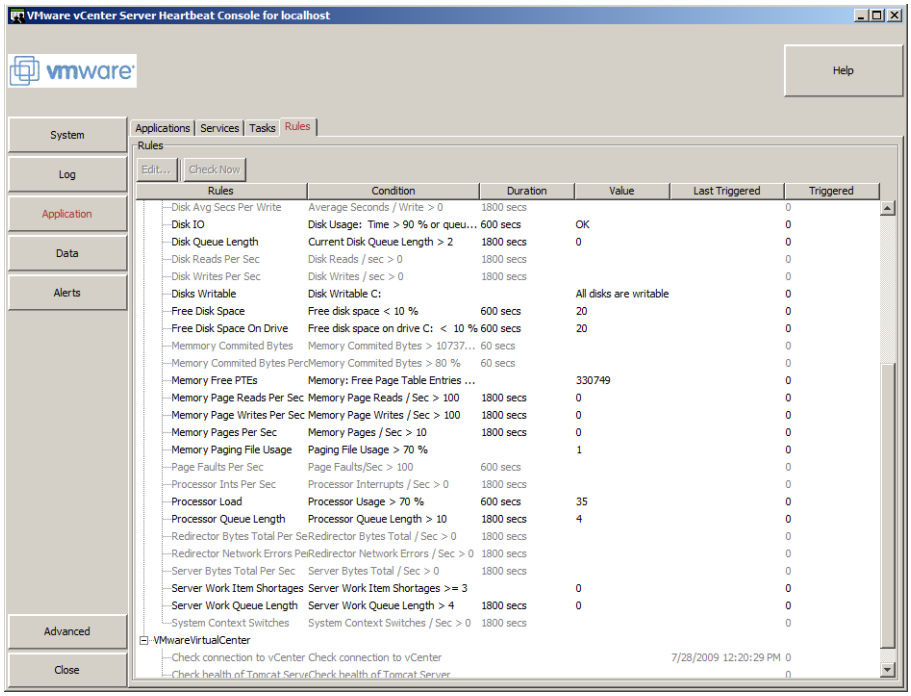
Checking a Rule Condition

To check a rule condition

1 Select the rule.

2 Click **Check Now**.

vCenter Server Heartbeat immediately checks the rule conditions of the current configuration against the attributes of the system or application.



Data Protection

11

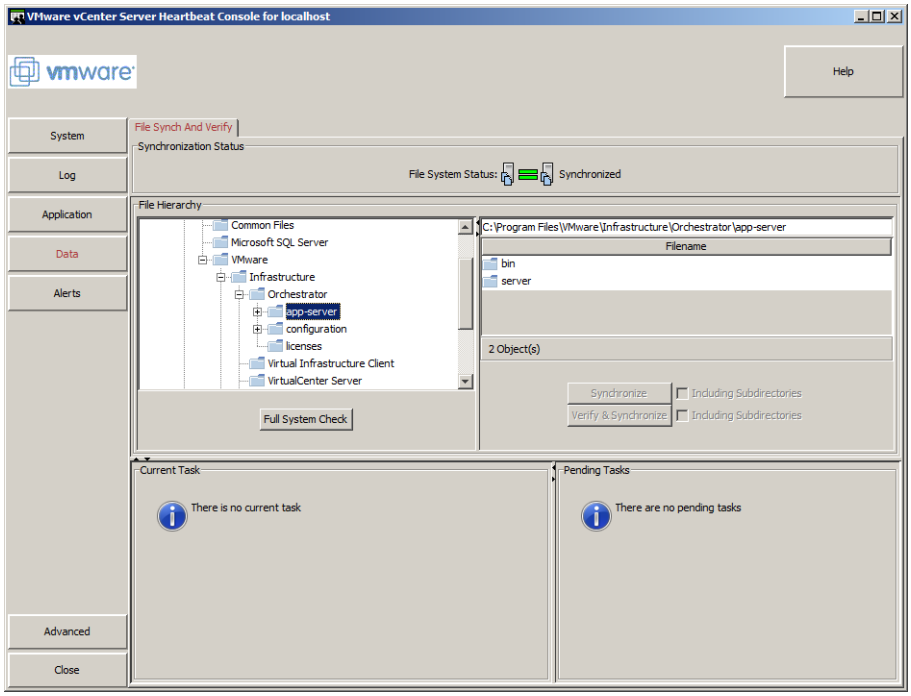
This chapter includes the following topics:

- "Data Protection Overview" on page 164
- "Automatic Filter Discovery" on page 164
- "Configuring Max Disk Usage" on page 167
- "Reviewing Status of Protected Files" on page 168
- "Determining Effective Filters" on page 168
- "Initiating File Synchronization Manually" on page 169
- "Initiating a Full System Check" on page 170
- "Reviewing the Registry Synchronization Status" on page 171
- "Initiating a Full Registry Check" on page 172

Data Protection Overview

The filter driver identifies files to protect and disk I/O operations to intercept and replicate on the passive server.

Use this driver to filter files for inclusion in or exclusion from the replication process.



vCenter Server Heartbeat protects a folder called `Protected` on the system partition.

You can configure the system to protect any permutation or combination of file structures on the active server by adding inclusion filters.

NOTE vCenter Server Heartbeat forbids replicating certain files and folders by using a veto. If an inclusion filter includes any of those files or folders, the entire filter is vetoed, even if an exclusion filter is used to prevent replication of those files and folders. Examples of folders are the `vCenter Server Heartbeat installation` directory or the `system32` folder.

The VMware application folder contains the active server (unsafe) and passive server (safe) queues on the active and passive servers. This folder must be explicitly excluded from file protection.

Automatic Filter Discovery

When Administrators make changes to the configuration, vCenter Server Heartbeat adjusts file filter protection for protected locations. Additionally, the SQL Server plug-in provides database protection including changes or additions to the database and log files.

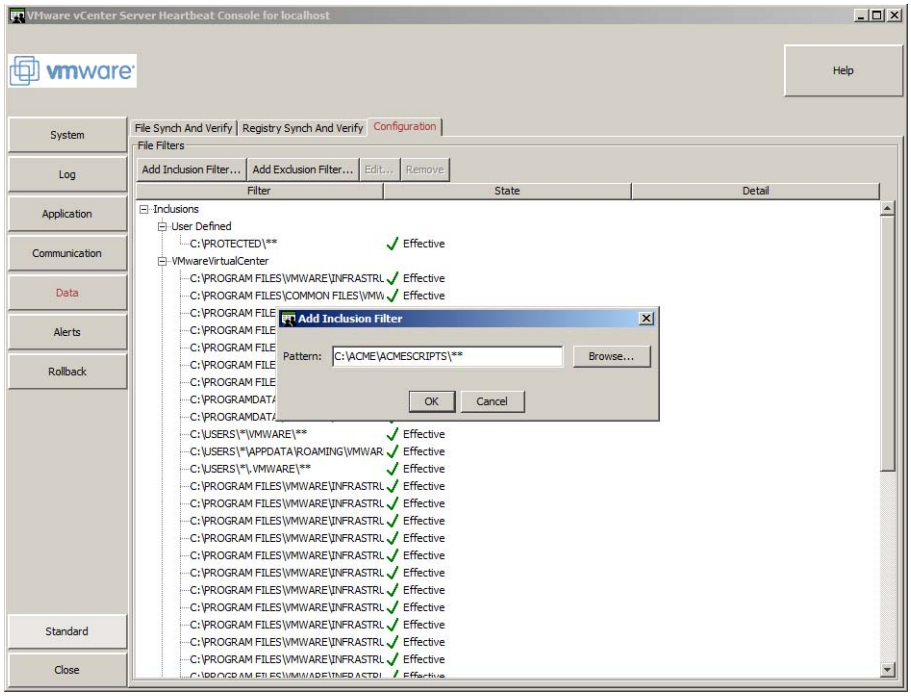
Adding a User-Defined Inclusion Filter

To add a user-defined Inclusion Filter

1 Click **Advanced** > **Data**.

2 Click the **Configuration** tab.

You can specify the Inclusion Filter on the **Data** page.



File Filters displays three columns: **Filter**, **State**, and **Detail**.

- **Filter** lists the pattern for protecting files and folders on the active server.
- **State** describes the filter state
  - **Effective** – The filter is properly configured and protects (replicates) the stipulated files to the passive server.
  - **Subset** – contained within another filter
  - **Not Effective** – not contained within another filter
- **Detail** describes file filter details based upon the state.

To define filters that protect user defined files and folders

1 Click **Add Inclusion Filter** and type the complete path and pattern, specify a pattern containing wildcards, or use **Browse** to locate the file or folder.

2 Click **OK**.

The two forms of wildcards available are *****, which matches all files in the folder, and ******, which matches all files, subfolders and the files in the subfolders of the folder.

After defining the filter, you can add additional Inclusion Filters.

3 To edit file filter definitions, select the filter and click **Edit**.

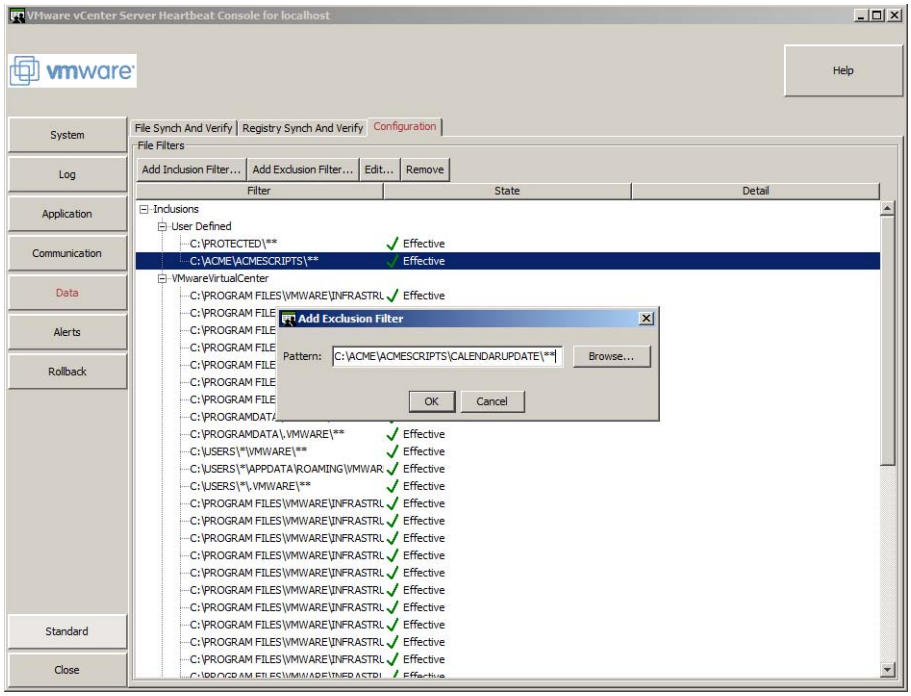
Adding a User-Defined Exclusion Filter

Exclusion Filters create a subset of an Inclusion Filter to specify items to exclude from protection.

To define filters that exclude files and folders from protection and replication

1 Click **Add Exclusion Filter** and type the complete path and pattern, specify a pattern containing wildcards, or use **Browse** to locate the file or folder.

2 Click **OK**.



The two forms of wildcards available are *****, which matches all files in the folder, and ******, which matches all files, subfolders and the files in the subfolders of the folder.

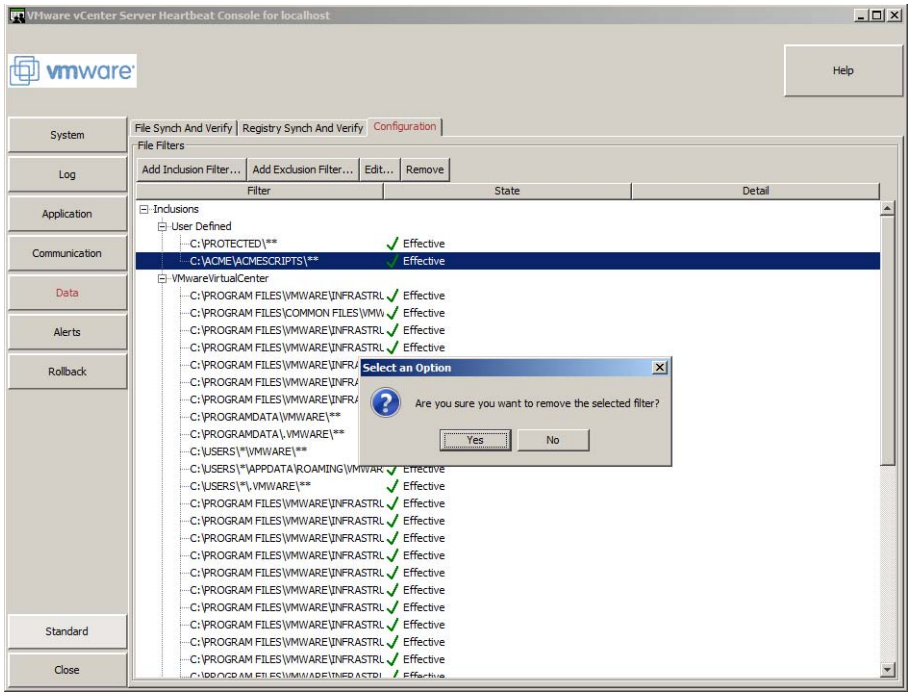
3 To edit file filter definitions, select the filter and click **Edit**.

Removing User-Defined Inclusion or Exclusion Filters

To remove an Inclusion or Exclusion Filter

1 Select the filter.

2 Click **Remove**.



Configuring Max Disk Usage

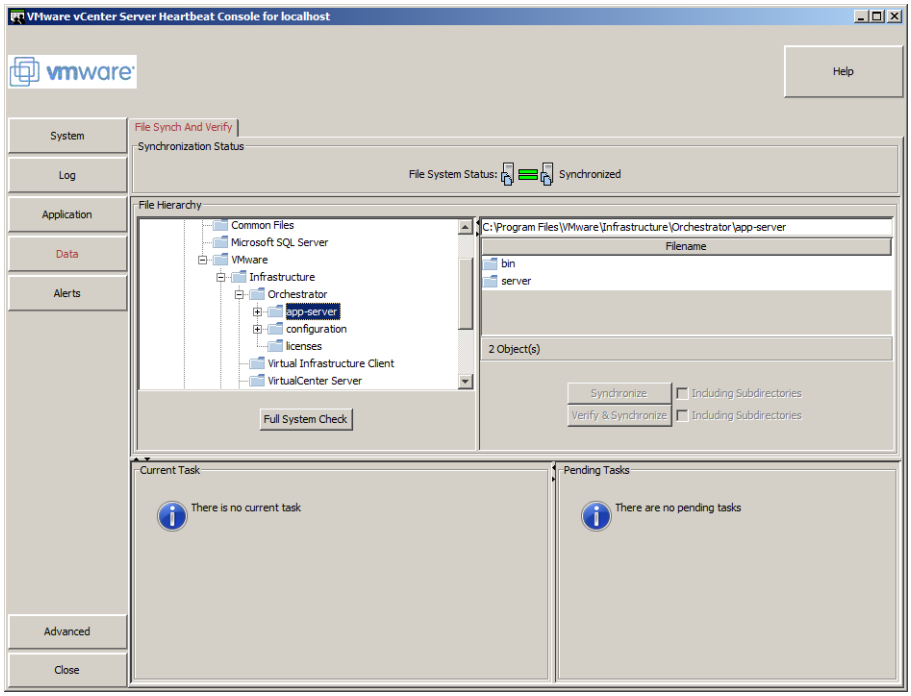
The active server (unsafe) and passive server (safe) queues are preconfigured to utilize a maximum space on disk of 1GB. If required, you can adjust the disk space.

1 Navigate **Advanced** > **Communications** > **Configuration** and select **Max Disk Usage**.

2 Consider increasing disk space when queued data requires more space during slow connectivity on VMware Channel.

Reviewing Status of Protected Files

Click the **File Sync and Verify** tab to review the status of protected files.



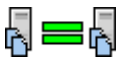
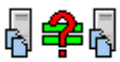
The **Synchronization Status** graphically displays the global status of the file synchronization and verification, with the same seven different states in the **System** page.

A tree structure graphically represents the protected files and folders as defined by the file filters. Expand or collapse each level by double-clicking the appropriate folder. The + icon next to a folder indicates the presence of subfolders.

The right side displays the subfolders, the protected files within folders and their synchronization status.

The synchronization status for each file can read three different values depending on the verification and synchronization states as described in Table 11-1.

Table 11-1. Synchronization Status

Icon	Description
	The file is verified and successfully synchronized.
	The file is not synchronized on the active and passive servers. This state often follows a failover and requires manual synchronization and verification.
	The file or folder has not been checked because a full system check has not been performed or the system check has not yet reached the file or folder.

Determining Effective Filters

An Effective Filter is the result of the remainder of the files and folders stipulated in the Inclusion Filter after removing the files and folders in the Exclusion Filter.

Filters are compared with each other, and if one filter is a superset of another, the superset filter is used. You can configure a single, general filter to replace file servers with 1000s of individual shares requested by a plug-in. The **Configuration** pane displays rejections after filters are validated before passing to the replication components.

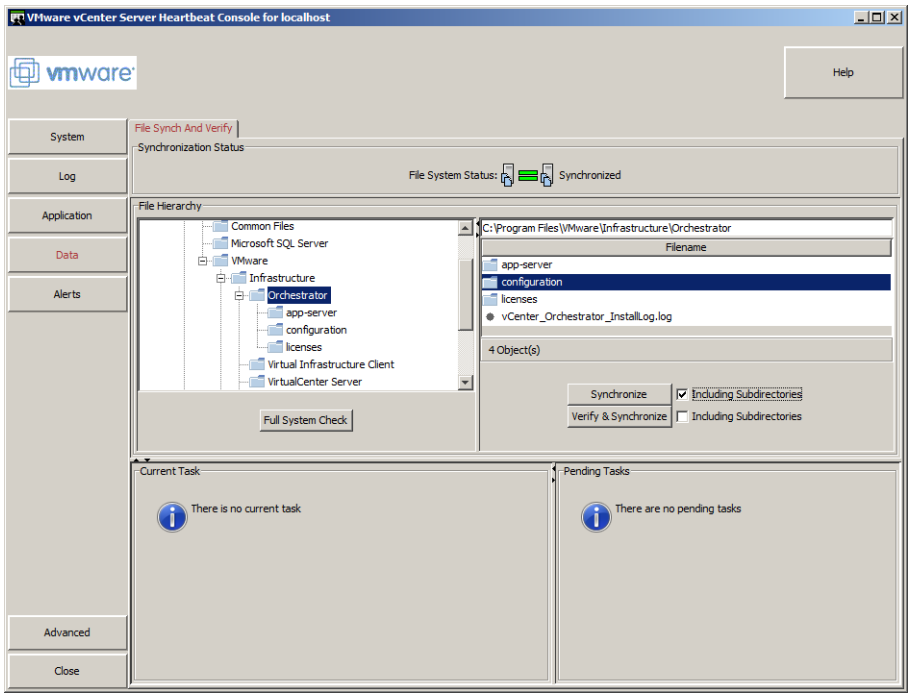
Initiating File Synchronization Manually

The **Data** page displays files that were detected as out of synchronization.

1 To manually synchronize the specified files, click **Synchronize**.

2 You can resynchronize files at any time. Select multiple files with the Shift or Ctrl keys and click **Synchronize**.

3 Select **Including Subdirectories** to synchronize files within folders.



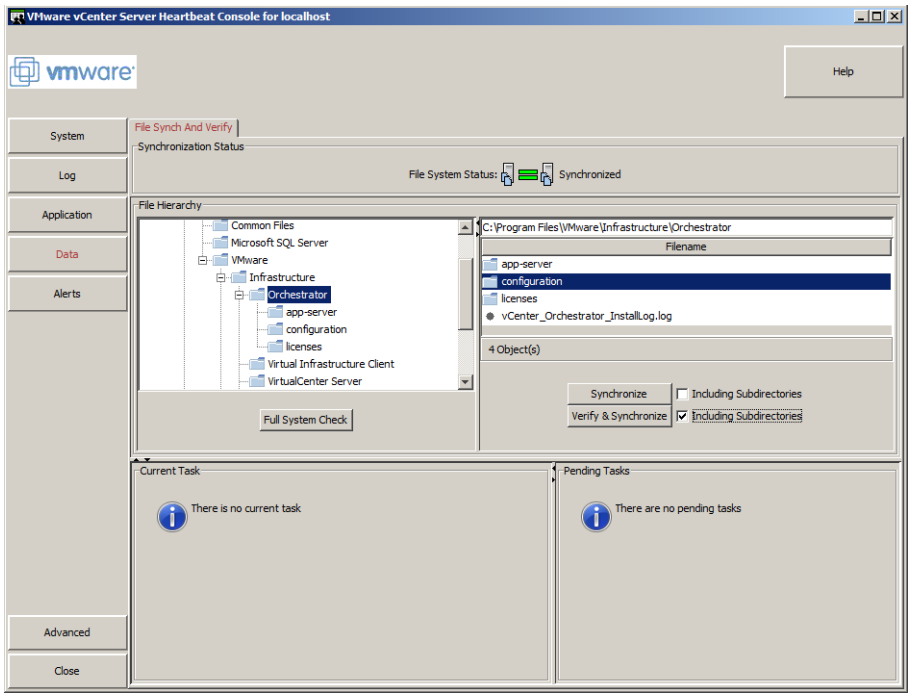
A progress graphic displays the status of the verification or synchronization operation. When complete, the status displays a green **Synchronized** icon.

Initiating Verify and Synchronize Manually

To verify and synchronize folders

1 Use **Verify & Synchronize** and select **Include Subdirectories** to ensure all underlying files and subfolders are included in the verification and synchronization operation.

2 Right-click a folder to access a popup menu to perform quick synchronization and verification of folders and subfolders.



A manual or scheduled synchronization and verification request is defined as a task that is queued for processing after the running task completes. Tasks display in the **Pending Tasks** pane. You can cancel individual tasks. If you cancel a scheduled task, you risk an unchecked system. Possible consequences of canceling tasks display in a warning message.

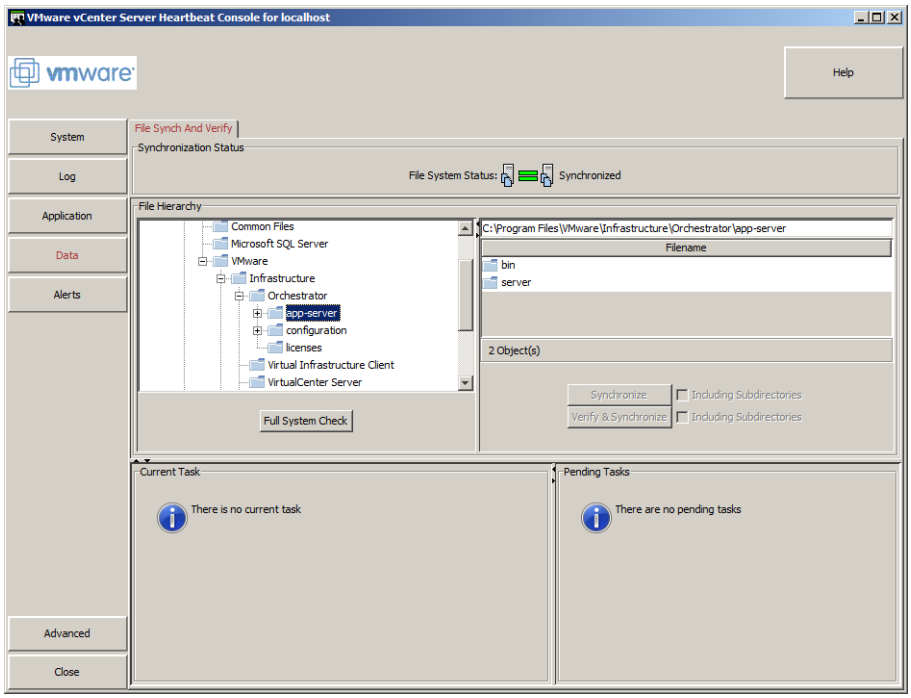
Initiating a Full System Check

You can verify and synchronize the entire protected file set with Full System Check. A Full System Check performs the same block level check of all the files set by the file filters in the initial startup synchronization and verification.

When you click **Full System Check**, a window asks you to confirm the request and warns you that depending on the amount of data under protection, this task can take a long time to complete (for example, a number of hours). Click **Yes** to perform the check.

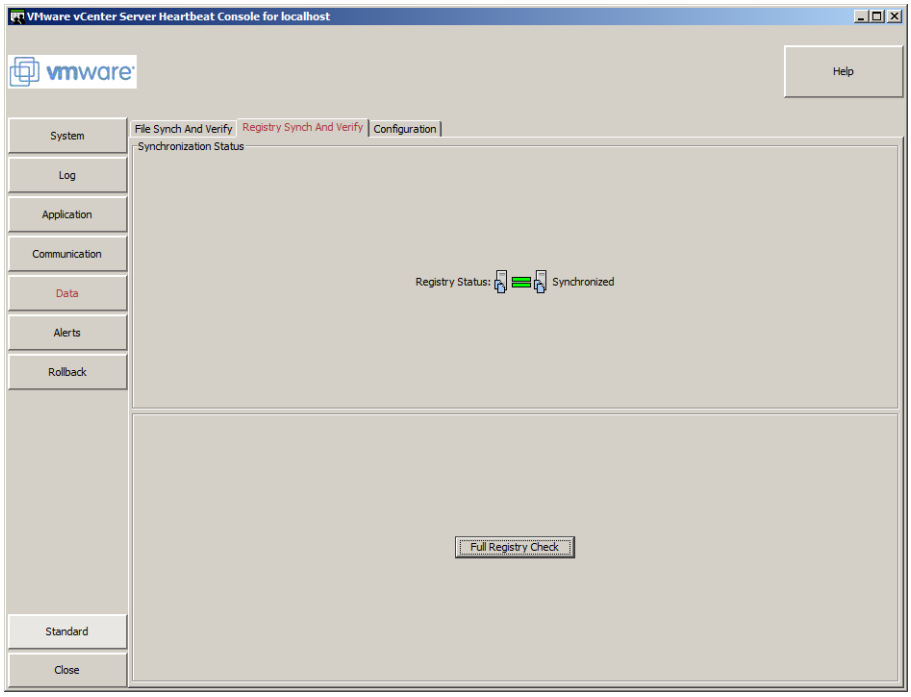
Switchover cannot occur until the full system check completes and the File System Status is **Synchronized**.

The File System Status is **Unchecked** when you cancel the task. Depending on the amount of data, resynchronization can take substantial time to complete.



Reviewing the Registry Synchronization Status

Use **Registry Sync and Verify** to review the status of registry replication.



The status of registry synchronization is displayed in Synchronization Status.

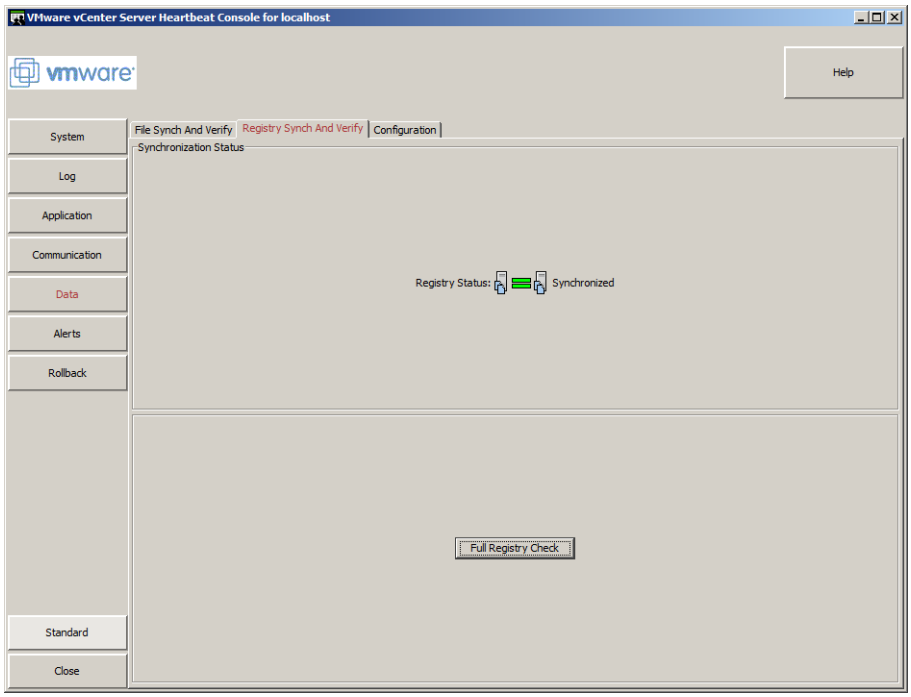
Full Registry Check rescans and synchronizes all the registry keys matching the built-in registry filters between the servers.

Initiating a Full Registry Check

To initiate a full registry check

1 Click **Data** in the navigation panel and click the **Registry Sync and Verify** tab.

2 Click **Full Registry Check**.



Other Administrative Tasks 12

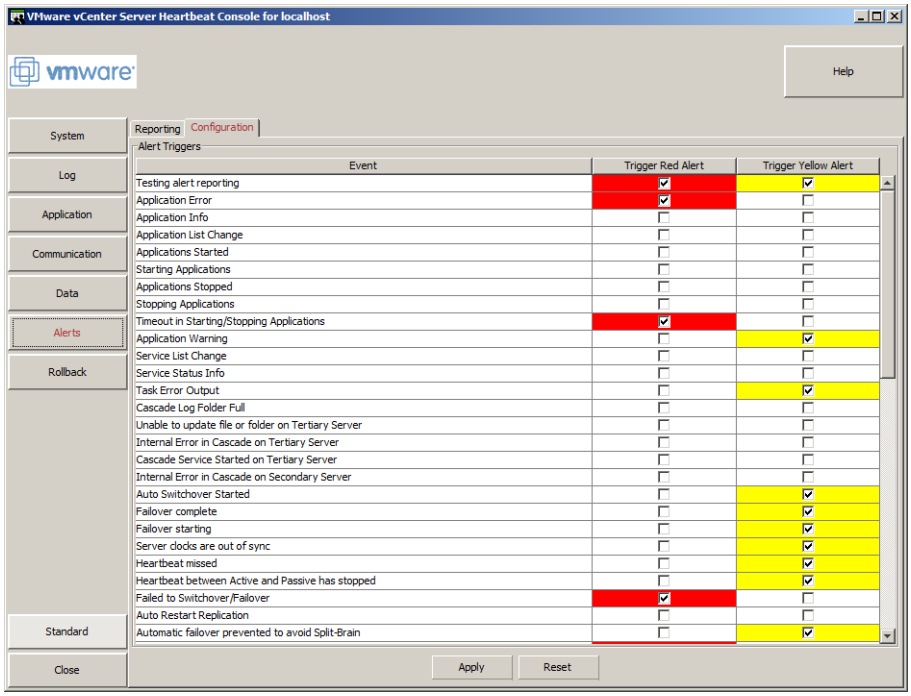
This chapter includes the following topics:

- "Configuring Alerts" on page 173
- "Configuring Alert Reporting" on page 174
- "Test Alert Reporting" on page 176
- "Configuring Event Log Files" on page 177
- "Reviewing Event Logs" on page 178

Configuring Alerts

vCenter Server Heartbeat can send predefined alerts to remote administrators by email using **Advanced** > **Alerts**.

You can configure alerts in the **Configuration** tab on the **Alerts** page.



You can configure two alert states: Red alerts are critical and yellow alerts are not as serious. These alerts are preconfigured with the recommended alerting levels.

To reconfigure each event to trigger red, yellow, or no alert, check the appropriate boxes and click **Apply**.

To reset the alerts to the last applied changes, click **Reset**.

Configuring Alert Reporting

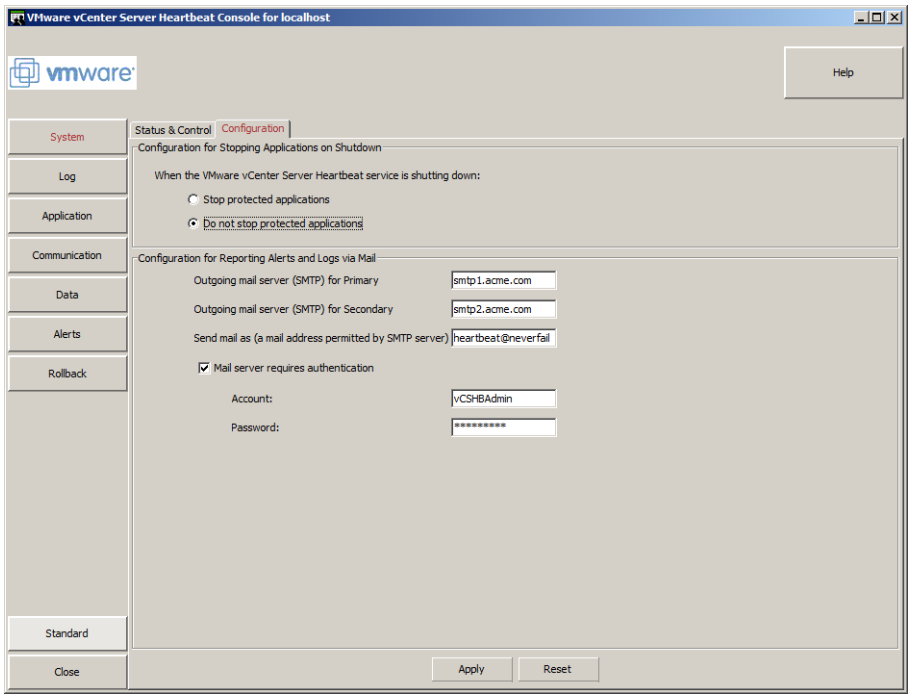
vCenter Server Heartbeat can alert the administrator and route logs by email when an Alert condition exists.

To configure email alerts

1 Click **Advanced** > **System** and click the **Configuration** tab.

2 Type the outgoing SMTP server of both the Primary server (when active) and the Secondary server (when active) in the appropriate fields.

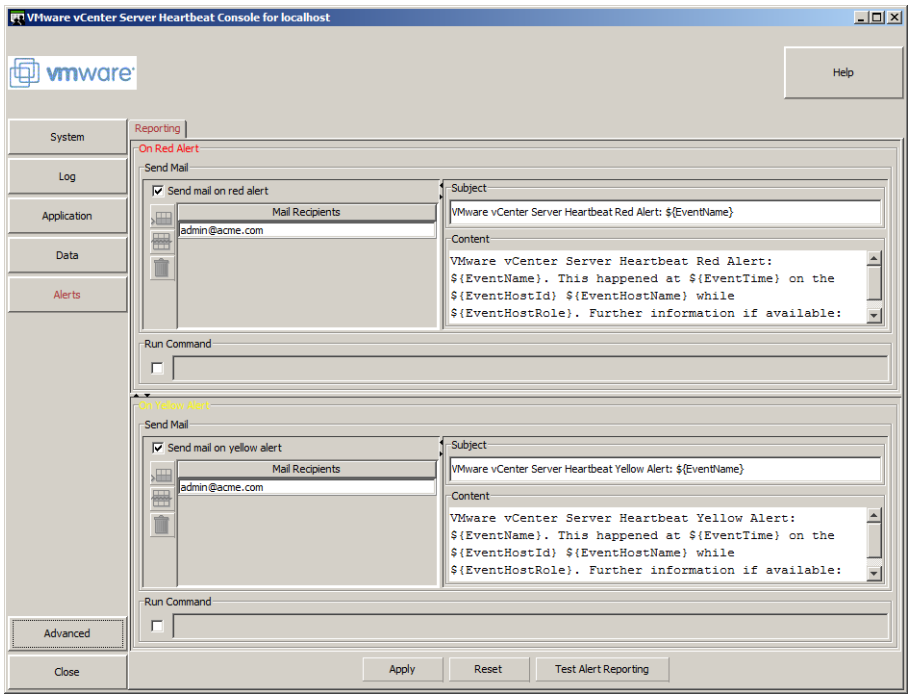
3 Type the FQDN of the mail server. Type an email address that is authorized to send mail through the SMTP server.



4 If the SMTP servers require authentication to accept and forward SMTP messages, select **Mail Server requires authentication** and specify the credentials for an appropriate authenticated user account.

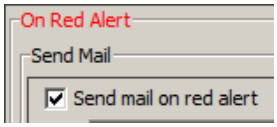
5 Click **Apply**. To restore the configuration to the last saved state, click **Reset**.

You can configure email recipients in the **Reporting** tab of the **Alerts** page after configuring the trigger levels and the email server.



Red or yellow alert triggers emails to the same or different recipients. The process to add recipients is the same for both trigger levels.

1 Select **Send mail on red alert** or **Send mail on yellow alert**.



2 Click **Add Row** and type a fully qualified email address for each recipient in each row for the respective trigger level alert.

3 To delete a row, click **Delete row**. To clear a trigger level, click the **Trash can** icon.

Use the preconfigured subject and content of the alert emails for both Red or Yellow alerts. You can add content as required. VMware recommends leaving the preconfigured subject and content and if necessary, add additional information.

Another method to send an alert notification is:

1 Select **Run Command** under the pertinent alert state.

2 **Browse** for a script to run or use a command line argument to run on the alert trigger.

The preconfigured WScript command creates an event in the Application Event Log and can be customized to include vCenter Server Heartbeat specific informational variables as detailed in Table 12-1.

Table 12-1. Script Variables

Variable	Value
$EventId	Id of event as listed above
$EventName	Human-readable name of event
$EventDetail	Detail message for event
$EventTime	Time at which event occurred

The following command line argument creates an event in the Application Event Log listing the machine that caused the alert, the time the alert occurred, the name, and details of the alert:

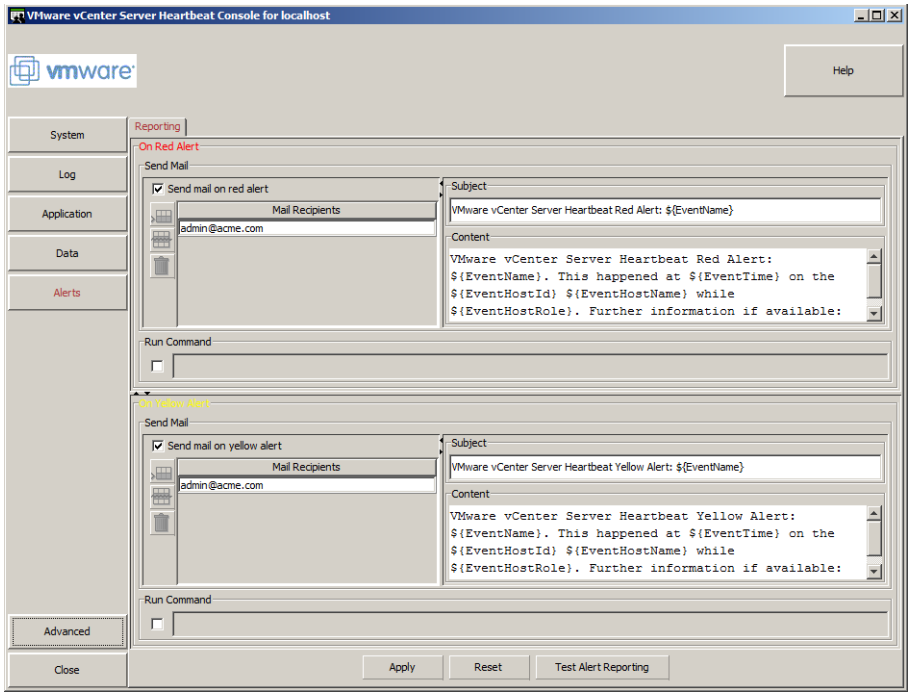
```
WScript //T:10 $(installdir)\bin\alert.vbs "VMware vCenter Server Heartbeat alert on
$EventHost at $EventTime because $EventName ($EventDetail). Event Id is $EventId"
```

3 Click **Apply** to save the changes and enforce the defined notification rules.

4 To restore the configuration to the last saved state, click **Reset**.

Test Alert Reporting

Click **Test Alert Reporting** to run a test alert email. This way you can avoid triggering an actual alert during the operation of the active server.

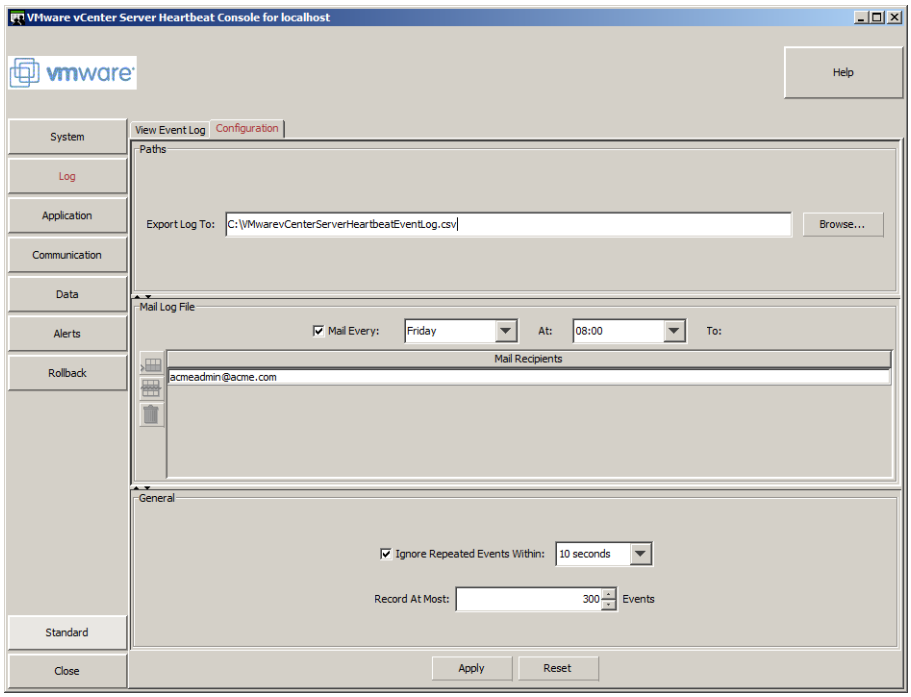


Configuring Event Log Files

To configure default settings for log files

1 Select **Advanced** > **Log**. Click the **Configuration** tab to define the filename and path of the exported comma-separated variable (CSV) file.

2 You can manually type a path and filename or use **Browse** and navigate the file. Click **Apply**.



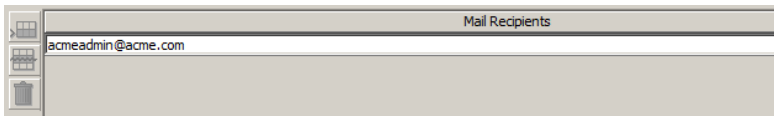
Configuring Log File Email Recipients

Use vCenter Server Heartbeat to email the log to specified personnel at predetermined intervals.

To configure email log notifications

1 To configure vCenter Server Heartbeat to email a copy of the log file, select **Mail Every,** and configure the day and time to send the log file.

2 Specify the recipients. Click the **Add Row** icon on the top left of the email recipient data grid and type the email address in the row.

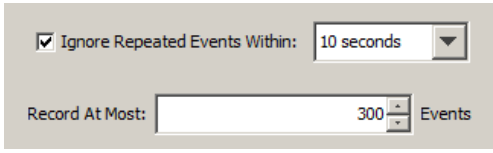


3 To remove a recipient, select the row and click the **Delete selected row** icon on the top left of the data grid.

4 To clear the entire data grid, click the **Trash can** icon.

5 You can configure additional features for event logs in the main **Configuration** page.

6 To override multiple logs generating for a single event, select **Ignore Repeated Events Within** and set the time increment to ignore the duplication.



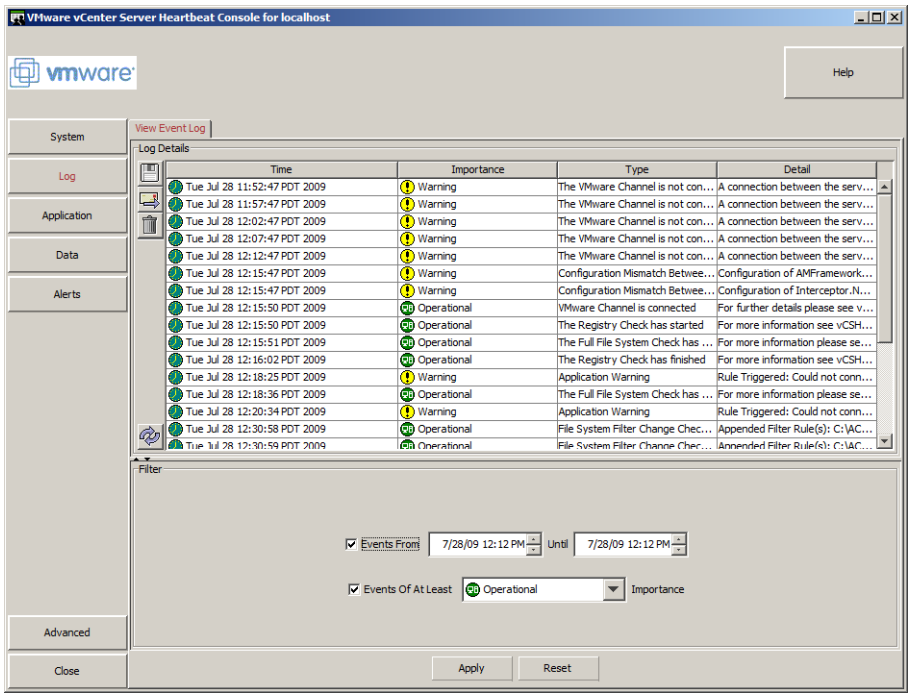
7 To adjust the length of the event log list, use **Record At Most**. The default length is 100 events, but you can customize this value.

8 Click **Apply** to commit the changes.

9 Click **Reset** to restore the previously applied log configuration. **Reset** does not affect the logs already recorded in the list.

Reviewing Event Logs

The **Log Details** data grid lists events logged chronologically by default.

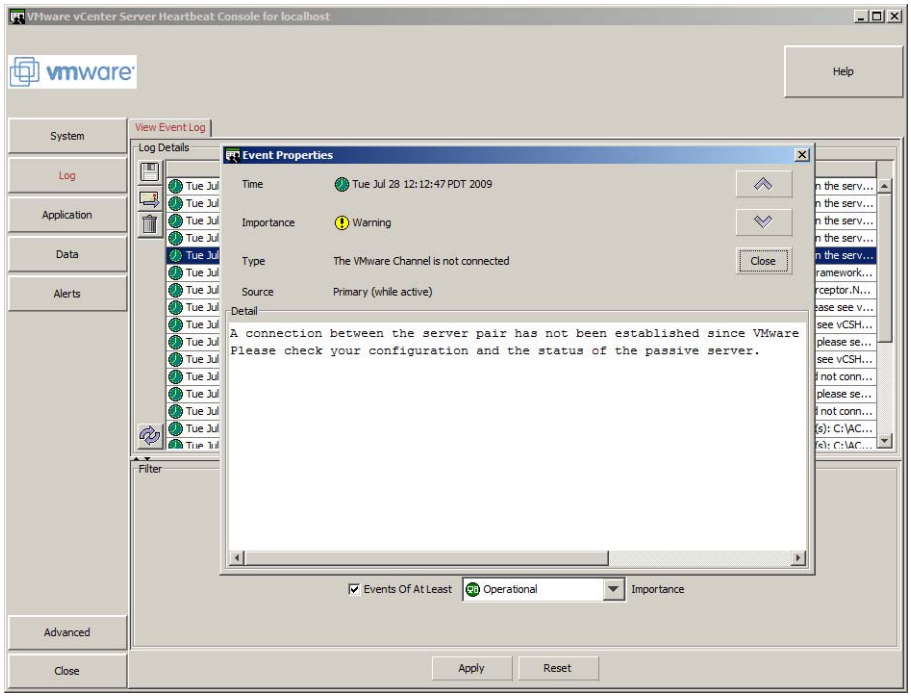

VMware vCenter Server Heartbeat Console for localhost
vmware
Help
System
Log
Application
Data
Alerts
Advanced
Close
View Event Log
Log Details
Time
Importance
Type
Detail
Tue Jul 28 11:52:47 PDT 2009 Warning The VMware Channel is not con... A connection between the serv...
Tue Jul 28 11:57:47 PDT 2009 Warning The VMware Channel is not con... A connection between the serv...
Tue Jul 28 12:02:47 PDT 2009 Warning The VMware Channel is not con... A connection between the serv...
Tue Jul 28 12:07:47 PDT 2009 Warning The VMware Channel is not con... A connection between the serv...
Tue Jul 28 12:12:47 PDT 2009 Warning The VMware Channel is not con... A connection between the serv...
Tue Jul 28 12:15:47 PDT 2009 Warning Configuration Mismatch Betwee... Configuration of AMFramework...
Tue Jul 28 12:15:47 PDT 2009 Warning Configuration Mismatch Betwee... Configuration of Interceptor.N...
Tue Jul 28 12:15:50 PDT 2009 Operational VMware Channel is connected For further details please see v...
Tue Jul 28 12:15:50 PDT 2009 Operational The Registry Check has started For more information see vCSH...
Tue Jul 28 12:15:51 PDT 2009 Operational The Full File System Check has ... For more information please se...
Tue Jul 28 12:16:02 PDT 2009 Operational The Registry Check has finished For more information see vCSH...
Tue Jul 28 12:18:25 PDT 2009 Warning Application Warning Rule Triggered: Could not conn...
Tue Jul 28 12:18:36 PDT 2009 Operational The Full File System Check has ... For more information please se...
Tue Jul 28 12:20:34 PDT 2009 Warning Application Warning Rule Triggered: Could not conn...
Tue Jul 28 12:30:58 PDT 2009 Operational File System Filter Change Chec... Appended Filter Rule(s): C:\AC...
Filter
Events From
7/28/09 12:12 PM
Until
7/28/09 12:12 PM
Events Of At Least
Operational
Importance
Apply
Reset

The logs show the time the event happened, its importance, the type of event that triggered the log, and its detail.

The data grid displays truncated information.

To review the details

1 Double-click the entry in the data grid.



Event Properties displays the full detail and trace of the log that caused the event and the source of the error to aid in troubleshooting.

2 Use the **Up** and **Down** arrows in this window to review other logs. This feature is useful where many logs have occurred simultaneously and helps to identify the source of the problem.

3 Click **Close** to close the **Event Properties**.

Table 12-2. Log Events

Icon	Description
	Errors within the underlying operation of vCenter Server Heartbeat and can be considered critical to the operation of the system.
	Warnings generated for discrepancies within the vCenter Server Heartbeat operational environment that are not deemed critical to the operation of the system.
	System logs are generated following normal vCenter Server Heartbeat operations. You can use these logs to verify the success of processes such as file synchronization.
	Information on operations within the graphical user interface rather than operations on vCenter Server Heartbeat service, such as login.

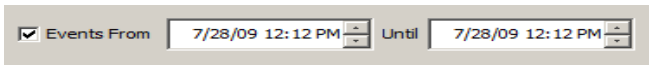
To display logs according to severity

1 Select **Events of at Least**.

2 Select the importance level and click **Apply** to display logged events equal to or greater than the selected severity.

You can filter logs to display a subset of logs between a specific date and time range.

3 Select **Events From**, adjust the start date, end date, and time, and click **Apply**.



4 Click **Reset** to remove and reset the filter criteria

Table 12-3. Log Configuration Icons

Icon	Purpose
	To refresh the list of events, click **Refresh Event Log** at the bottom left of the **Log Details** data grid.
	To clear the list, click **Remove all Entries** at the top left of the **Log Details** data grid.
	To export the list to a comma-separated variable file, click **Export event log** at the top left of the **Log Details** data grid. You can configure the filename and path to export the data in the **Configuration** tab.
	To immediately email the list, click **E-mail**.

Troubleshooting 13

This chapter includes the following topics:

- "Troubleshooting Unexpected Behaviors" on page 181
- "Two Active Servers" on page 181
- "Two Passive Servers" on page 183
- "Synchronization Failures" on page 184
- "Registry Status is Out of Sync" on page 186
- "Channel Drops" on page 186
- "Subnet or Routing Issues " on page 190
- "MaxDiskUsage Errors" on page 190
- "MaxDiskUsage Error Messages" on page 191

Troubleshooting Unexpected Behaviors

The following unexpected behaviors illustrate symptoms, causes and resolution for a given scenario.

Two Active Servers

When two identical active servers are live on the same network, vCenter Server Heartbeat refers to the condition as split-brain syndrome. Two active servers do not occur by design and when detected, must be resolved immediately.

Symptoms

Split-brain syndrome is identified by the following symptoms:

- Both servers in the pair are running and in an active state. The task bar icons display **P / A** (Primary and active) and **S / A** (Secondary and active).
- An IP address conflict occurs on a server pair running vCenter Server Heartbeat on the Principal (Public) IP address.
- A name conflict occurs on a server pair running vCenter Server Heartbeat. In a WAN environment the Primary and Secondary servers connect to the network using different IP addresses. However, if the servers are running with the same name and are visible to each other across the WAN, a name conflict occurs.
- Clients (for example, Outlook) cannot connect to the server running vCenter Server Heartbeat.

Causes

The most common causes of two active servers (Split-brain syndrome) are as follows:

- Loss of the VMware Channel connection (most common in a WAN environment)
- The active server is too busy to respond to heartbeats
- Incorrect configuration of the vCenter Server Heartbeat software

You must determine the cause of the Split-brain syndrome and resolve the issue to prevent this condition from recurring.

Resolution

To resolve a Split-brain syndrome, identify the server with the most up-to-date data. If you identify the wrong server you risk losing data. You must reinstate the correct server.

To identify the server with the most up-to-date data

1 Check the date and time of files on both servers. Make the most up-to-date server the active server.

2 From a client PC on a LAN, run `nbtstat –A 192.168.1.1` where the IP address is the Principal (Public) IP address of the server. This can help identify the MAC address of the server currently visible to client machines.

NOTE If both active servers were servicing clients, perhaps at different WAN locations, you can make only one server active. Both servers contain recent data that cannot be merged using vCenter Server Heartbeat. To restart replication, make one server active and one server passive. When replication restarts, the active server overwrites all data on the passive server. You can manually extract the up-to-date data from the passive server prior to restarting replication. Consult the Microsoft knowledge base for information on various tools for this purpose. For further information, contact your VMware support representative.

To resolve two active servers (Split-brain syndrome)

1 Identify the server with the most up-to-date data or the server to make active.

2 Shut down vCenter Server Heartbeat on both servers (if running).

3 On the server to make passive, right-click the **Task bar** icon, and select the **Server Configuration** wizard.

4 Click the **Machine** tab and set the server role to **passive**. Do not change the identity of the server (Primary or Secondary).

5 Click **Finish** to accept the changes.

6 Restart this server.

7 Start vCenter Server Heartbeat, if required, and check that the Task bar icon now reflects the changes by showing **P / -** (Primary and Passive) or **S / -** (Secondary and Passive).

8 On the active server, right-click the **Task bar** icon and select the **Server Configuration** wizard.

9 Click the **Machine** tab and verify that the server role is set to **active**. Do not change the identity of the server (Primary or Secondary).

10 Click **Finish** to accept the changes.

11 Restart this server. As the server restarts, it connects to the passive server and starts replication. The active server overwrites data on the passive server.

12 Start vCenter Server Heartbeat, if required, and check that the Task bar icon now reflects the changes by showing **P / A** (Primary and active) or **S / A** (Secondary and active).

13 Log in to the vCenter Server Heartbeat Console.

14 Check that the servers have connected and replication has started.

Two Passive Servers

Primary and Secondary servers are both passive at the same time. This situation is serious and must be resolved immediately.

Symptom

You are unable to connect to protected applications, and if you configured alerts, you receive notification that replication is not functioning properly.

Causes

The condition of two passive servers results from a sudden failure on the active server. Examples:

- An unexpected termination of the Neverfail Server R2 service
- A transient power failure
- A server reset triggered from the Power or Reset button
- An unclean shutdown. Following an unclean shutdown, an active server assumes the passive role to isolate itself from the network until the failure is investigated.
- The active server fails before the handshake that establishes the VMware Channel connection. The passive server cannot detect that the active server is not responding when the failure occurs and cannot determine the condition of the active server. The active server suffers a transient failure and the passive server cannot respond by failing over into the active role, leaving both servers in the passive role.
- Both Primary and Secondary servers experience a power outage simultaneously, for example, they use the same power source and neither is attached to a UPS. A failover cannot occur and when the servers are restarted, each displays the following error message:

  ```
  Cannot start replication because previous run did not shutdown properly. Check configuration.
  ```

NOTE If you attempt to start vCenter Server Heartbeat without reconfiguring one server in the pair as active, vCenter Server Heartbeat responds with the following warning:

```
[U16] Serious configuration mismatch between the two servers. Please reconfigure so there is one and only one Primary, and one and only one Active.
```

Resolution

Two passive servers prevent users from accessing the protected application and should be resolved immediately.

To resolve two passive servers

1 Determine the active server.

2 Shut down vCenter Server Heartbeat on both servers. Leave any protected applications running on the server to make active.

3 On the server to make active, start the **Server Configuration** wizard, and select the active role. Do not change the identity (Primary or Secondary).

4 On the server to make passive, start the **Server Configuration** wizard, and confirm the passive server. Do not change the identity (Primary or Secondary).

5 Restart the passive server. All protected application services stop.

6 Start vCenter Server Heartbeat on both servers.

Synchronization Failures

When you start vCenter Server Heartbeat, a full system check occurs to verify the following:

- All protected registry keys and values from the active server are present on the passive server.
- All protected file and folder structures from the active server are present on the passive server.

After the full system check completes, the File System Status and the Registry Status display as **Synchronized**. However, the File System Status or the Registry Status can also display as **Out of sync** or **Synchronized and busy processing**. Some typical scenarios are described with possible causes and workarounds.

Services Running on the Passive Server

Services running on a passive server is not normal behavior and can prevent synchronization.

Symptom

File System Status is **Out of sync** or **Synchronized and busy processing**.

Cause

A service running on the Passive server opens a protected file for exclusive access. If vCenter Server Heartbeat attempts to update this opened file, the Apply component logs the following error message:

[N29]The passive VMware vCenter Server Heartbeat server attempted to access the file: {filename}. This failed because the file was in use by another application. Please ensure that there are no applications which access protected files running on the passive.

NOTE This occurs if the vSphere Client is left running on the passive server.

Services that keep files locked on the passive server are:

- Protected application services
- File level antivirus tool services

NOTE vCenter Server Heartbeat periodically checks for and stops any services running on the passive server.

Resolution

Until the file is closed on the passive server, vCenter Server Heartbeat reports the file status and the File System Status as **Out of sync**.

To resolve the Out of sync status

1. Set Protected Application services to **Manual** on both servers and verify that they are not running on the passive server.
2. Set Recovery Actions to **Take No Action**. You can set this from the Service Control Manager (SCM) for the Protected Application services. Otherwise, the SCM restarts the Protected Application services.
3. Verify that file level antivirus is not part of the protected set as the file level antivirus and the corresponding services are running on both machines.

VMware Channel Incorrectly Configured

If the VMware Channel is not properly configured, it cannot initiate the handshake to establish communications through the VMware Channel connection.

Symptom

Failure to establish the VMware Channel connection prevents a full system check, thereby leaving the File System Status and Registry Status as **Out of sync**.

Causes

The most common VMware Channel configuration errors are as follows:

- VMware vCenter Server Heartbeat Packet Filter is enabled on one or more VMware Channel NICs
- VMware Channel IP addresses are configured in different subnets
- In a WAN implementation, no static routes exist between the VMware Channel NICs

Resolution

The VMware Channel configuration should be reviewed to verify proper configuration.

To resolve a VMware Channel configuration error

1 Disable the VMware vCenter Server Heartbeat Packet Filter on VMware Channel NICs.

2 Configure the VMware Channel IP addresses properly.

3 In a WAN implementation, configure static routes between VMware Channel NICs properly.

4 Disable NetBIOS on the VMware Channel NICs.

Incorrect or Mismatched Disk Configuration

When vCenter Server Heartbeat starts, it checks the complete set of file filters for consistency.

Symptom

If any of the entries points to a non-existent drive letter or to a non-NTFS partition, the list of file filters resets to the default value of `C:\Protected\**`. This is a safety measure as vCenter Server Heartbeat requires the same drive letter configuration on the Primary and the Secondary servers, and only supports protection of NTFS partitions.

Cause

Different partition structures on Primary and Secondary servers, such that one or more file filters point to drives that cannot be protected on both servers. For example:

- The Primary server has drive G, a valid NTFS partition, but no corresponding drive exists on the Secondary server.
- The Primary server has drive G, a valid NTFS partition. The equivalent drive on the Secondary server is a CD or DVD drive, or a FAT or FAT32 partition that cannot be protected.

In either scenario, if you configure a file filter to protect a directory on drive G, the entire filter set is rejected and the filters are reset to the default value of `<Windows drive>\Protected\**`.

Resolution

Follow the steps documented in knowledge base article 1008458 (*vCSHB-Ref-500) Troubleshooting a set of File Filters that is reset to C:\Protected**.

Passive Server Has Less Available Space than Active Server

Inadequate available disk space on the passive server can cause replication to cease.

Symptom

Replication stops with the following error:

[N27]Failed to write information for the file: {filename} to the disk. Either the disk is full or the quota (for the SYSTEM account) was exceeded.

Cause

The passive server has less available disk space than the active server, preventing updates from being replicated to the passive server. The quantity of updates from the active server exceeds the passive server's available disk space.

Resolution

Free up some additional disk space on the passive server. Do not delete data from the protected set to prevent data loss in the event of a switchover. You could update the disk subsystem on the passive server. After allocating space, start replication.

Registry Status is Out of Sync

The Registry can be reported as **Out of sync** when one or more Registry keys fail to synchronize.

Resource Issues

Inadequate resources can cause poor performance and prevent the registry from synchronizing.

Symptom

vCenter Server Heartbeat logs the following error message:

```
Call to RegOpenKeyEx failed: on <Reg_Key>: Insufficient system resources exist to complete the requested service.
```

Cause

One or both of the servers are running low on virtual memory.

Resolution

Restart the server to free up virtual memory.

Registry Security Issues

Inability to access the registry prevents replication of the registry.

Symptom

vCenter Server Heartbeat is unable to read, sync, or replicate the registry.

Cause

If a protected registry key has permissions that deny Write access to the System account, this can prevent vCenter Server Heartbeat from synchronizing or replicating it.

Resolution

Change the permissions on the affected registry key to grant the System account Full Control.

Channel Drops

When the VMware Channel loses connection between the servers, the following scenarios can occur.

Performance Issues

Poor performance can be experienced as a result of a channel loss.

Symptom

The message `java.io.IOException: An existing connection was forcibly closed by the remote host` appears in the active server's `NFLog.txt` file, and the VMware Channel connection between the servers is lost.

Causes

This unusual condition points to an application or Windows experiencing a fault on the passive server. A sudden restart of the passive server can occur due to the following causes:

- The server is configured for automatic software update management and some updates force the server to restart
- A software or Operating System issue that occasionally fails and requires a system restart
- The Neverfail Server R2 service experiences problems, does not respond, or terminates unexpectedly

Resolution

To resolve the issue, make the following checks.

- Determine the likely source by examining the Windows event logs.
- If the server does not display evidence of a system restart or unresponsive application, one or both of the VMware Channel NICs could be forcing a channel disconnection. See "Hardware or Driver Issues on VMware Channel NICs" on page 187 for more information on this topic.

Passive Server Does Not Meet Minimum Hardware Requirements

Inadequate hardware can cause channel drops and result in poor performance.

Symptom

The data rate between the servers is very fast during a Full System Check and the VMware Channel drops.

Cause

The passive server does not meet the recommended hardware requirements for vCenter Server Heartbeat or it meets the requirements, but is much less powerful than the active server. The underpowered server cannot apply the received replication data from the active server at the rate that the data is sent to the passive server.

Resolution

To avoid reinstalling vCenter Server Heartbeat, upgrade the hardware, such as memory or CPU, on the passive server. Establish the identity (Primary or Secondary) of the affected server before you perform the upgrade.

Hardware or Driver Issues on VMware Channel NICs

NIC malfunctions and old or incorrect drivers can cause channel drops resulting in poor performance.

Symptom

The VMware Channel intermittently drops or disconnects and reconnects.

Causes

The following are common causes of NIC problems.

- Old or incorrect VMware Channel NIC drivers
- Hardware failure of the hub or Ethernet switch used for the VMware Channel connection
- Defective Ethernet patch or crossover cables

- Improper configuration of the NICs used for the VMware Channel connection
- ISP problems in a WAN environment

Resolution

When a NIC problem is encountered, the following should be checked.

- Verify that VMware Channel NIC drivers are the correct and latest versions. Known issues are identified with HP/Compaq ProLiant NC67xx/NC77xx Gigabit Ethernet NICs. Check other NIC types. See knowledge base article 1008383 (*vCSHB-Ref-116) – VMware vCenter Server Heartbeat and Gigabit Ethernet NIC drivers. (NC77XX)*.
- Verify hubs and Ethernet switches are operating properly. Identify and replace any defective components.
- Test for defective Ethernet patch or crossover cables and replace if defective.
- Correctly configure the NICs used for the VMware Channel connection.
- Check the physical link for ISP problems.

Firewall Connection

In a LAN or WAN deployment, the VMware Channel can be connected through one or more Internet firewalls. Because firewalls block unauthorized network traffic, configure firewalls on the route of the VMware Channel to allow channel traffic.

Symptoms

The VMware Channel cannot connect, or continuously connects and disconnects.

Causes

In a WAN deployment, port 57348 or any other port configured for the VMware Channel is closed on one or more firewalls on the route between the VMware Channel NIC on the Primary server and its counterpart on the Secondary server.

Resolution

Open port 57348 and any other port configured for the VMware Channel on all firewalls on the route between the VMware Channel NIC on the Primary server and its counterpart on the Secondary server.

Incorrect VMware Channel Configuration

An incorrectly configured channel connection can prevent proper communication and replication.

Symptoms

The following problems are experienced:

- IP conflicts occur on one of the VMware Channel IP addresses
- The VMware Channel does not connect, or connects and disconnects

Causes

The list below provides the most common misconfigurations.

- Identical IP addresses at each end of the VMware Channel
- IP addresses in different subnets without static routing at each end of the VMware Channel
- VMware Channel NIC configured for DHCP when a DHCP server is not available

During installation, vCenter Server Heartbeat configures the VMware Channel NICs with user-provided information. Incorrect information or incorrectly modifying the VMware Channel NIC configuration after installation causes the VMware Channel to fail communicating.

On rare occasions, if the Primary and Secondary servers have NICs of the same type in a different order, both the name and IP address of a VMware Channel NIC on the Primary server can transfer to the Principal (Public) NIC on the Secondary or the name and IP address of the Principal (Public) NIC can transfer to a VMware Channel NIC. Similarly, the names of the VMware Channel NICs can reverse on the Secondary server. You must reconcile the names of the NICs with their physical identities and assign the correct IP address to each NIC on the Secondary server.

Resolutions

The installation process manually assigns the correct IP addresses to each NIC on the Secondary server. If no VMware Channel connection occurs between the servers, verify the configuration of the IP addresses on the Secondary server's channel NICs. Check the settings for the Principal (Public) NIC. The configuration error can remain unrecognized until you perform a switchover or a failover occurs.

To capture the identities of all of the NICs on the Secondary server prior to installing vCenter Server Heartbeat, open a Windows Command Prompt on that server and execute the following command:

```
ipconfig /all > ipconfig.txt
```

The output of this command saves the name, TCP/IP configuration, and MAC address of each NIC on the Secondary server to a file called ipconfig.txt, which is present on that server after the PnP phase of the vCenter Server Heartbeat install completes. Compare the pre-install and post-install state of each NIC by running `ipconfig /all` from a Windows command prompt and compare the output of this command with the content of ipconfig.txt.

The MAC address of each NIC is connected to the physical identity of each card and never changes. You can identify each NIC by its MAC address and determine its original name and network configuration, even if this was updated by the PnP process.

VMware vCenter Server Heartbeat Packet Filter Is Enabled on the Channel NIC(s)

Proper configuration requires that the packet filter be disabled on the VMware Channel NIC. When the packet filter is enabled on the channel NICs, the following symptoms are encountered.

Symptom

Interference with network traffic across the VMware Channel results in an intermittent channel connection or no channel connection at all.

Cause

During installation, the VMware vCenter Server Heartbeat Packet Filter is installed and enabled on all NICs on both the Primary and Secondary servers. The Packet Filter on the VMware Channel NICs on each server is disabled later in the installation of vCenter Server Heartbeat. If the vCenter Server Heartbeat Packet Filter is left enabled on one or more channel NICs after installation completes, it can interfere with network traffic across the VMware Channel.

Resolution

Click the **Properties** tab for each Channel NIC on both servers and verify that the check box for **vCenter Server Heartbeat Packet Filter** is cleared, so that the Packet Filter is disabled on that NIC.

Subnet or Routing Issues

In a LAN or WAN deployment, the following connection problems can occur.

LAN Deployment

Incorrectly configured subnets or routing can cause channel problems resulting in poor performance or failure to connect.

Symptom

The Channel disconnects or fails to connect in a LAN deployment.

Causes

The Channel disconnects or fails to connect due to the Principal (Public) NIC and/or one or more channels sharing the same subnet.

Resolution

If vCenter Server Heartbeat is deployed in a LAN environment, the Principal (Public) IP address and the Channel IP address on a server must be in separate subnets. When multiple redundant channels are present, each must have its own subnet. Check the network configuration for each NIC on both servers in the pair and correct any issues.

WAN Deployment

Incorrect routing can prevent the active and passive servers from connecting in a WAN environment.

Symptom

The VMware Channel disconnects or fails to connect in a WAN deployment.

Cause

When the VMware Channel disconnects or fails to connect in a WAN deployment, the static route might not be configured or might be configured incorrectly.

When vCenter Server Heartbeat is deployed in a WAN, the Principal (Public) IP address and the VMware Channel IP addresses cannot be in different subnets, because there usually is a single network path between the two servers. Configure a static route between the endpoints to route traffic in the VMware Channel.

Resolution

Refer to knowledge base article 1008451 (*vCSHB-Ref-466) - Creating a static route for the VMware Channel Connection Where the Channel and Principal (Public) IP Addresses are on the Same Subnet in a WAN Environment* for a detailed discussion about WAN channel routing issues, and for instructions on configuring a static route for the VMware Channel.

MaxDiskUsage Errors

vCenter Server Heartbeat uses queues to buffer the flow of replication data from the active server to the passive server. This configuration provides resilience in the event of user activity spikes, VMware Channel bandwidth restrictions, or VMware Channel drops across a WAN deployment. Some types of file write activity also require buffering as they can cause a sharp increase in the amount of channel traffic. The queues are called the active server (unsafe) queue or the passive server (safe) queue.

Active Server (Unsafe) Queue

vCenter Server Heartbeat considers the active server queue as unsafe because the data in this queue has not yet been replicated across the VMware Channel to the passive server and therefore could be lost in the event of a failover. As a result of failover, some data loss is inevitable, with the exact amount depending on the relationship between available VMware Channel bandwidth and the required data transmission rate. If the required data transmission rate exceeds available VMware Channel bandwidth, the active server queue fills. If the available VMware Channel bandwidth exceeds the required data transmission rate, the active server queue empties. This situation is most commonly seen in a WAN environment, where VMware Channel bandwidth is restricted. In a LAN that normally has high bandwidth on a dedicated channel, the size of the active server queue is zero or near zero most of the time. On a server not protected with vCenter Server Heartbeat, all data is technically unsafe and subject to loss if the server fails.

Passive Server (Safe) Queue

The passive server queue is considered safe because the data in this queue already was transmitted across the VMware Channel from the active server, and is not lost in the event of a failover, which applies all updates to the passive server as part of the process.

Both active and passive server queues are stored on disk by default in the `<VMware vCenter Server Heartbeat Install Directory>\R2\log directory`, with a quota configured for the maximum permitted queue size (by default, 1GB on each server). You can configure both the queue location and the quota.

Two methods to set the queue size:

- Start vCenter Server Heartbeat, open the **vCenter Server Heartbeat Console**, and select **Advanced** > **Communication** > **Configuration**. Set the **Max Disk Usage** value and click **Apply**. Shut down and restart vCenter Server Heartbeat for the change to take effect. You are not required to stop protected applications.
- Open the **Server Configuration** wizard and click the **Logs** tab. Set the **Maximum Disk Usage** value and click **Finish**.

NOTE vCenter Server Heartbeat is a symmetrical system and can operate with either server in the active role. For this reason, the queue size is always set to the same value for both servers.

MaxDiskUsage Error Messages

The following error messages display when available disk space on the servers is exceeded.

[L9]Exceeded the Maximum Disk Usage (VCChannelExceededMaxDiskUsageException)

This message indicates that you have exceeded the amount of allocated disk space reserved for the queue.

Symptom

vCenter Server Heartbeat exceeds its preconfigured queue size.

Causes

On the active server, the size of the active server queue has exceeded the disk quota allocated for it. On the passive server, the size of the passive server queue has exceeded the disk quota allocated for it.

Resolution

While neither condition is critical, determine the sequence of events that led to the condition.

[L9]Exceeded the Maximum Disk Usage on the ACTIVE Server

This message indicates that you have exceeded the amount of allocated disk space reserved for the active server (unsafe) queue.

Symptom

Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from the active server.

Causes

A temporary interruption in the VMware Channel, or insufficient VMware Channel bandwidth to support the volume of replication traffic starts filling the active server queue. The size of the queue eventually exceeds the configured disk quota.

Resolution

Assuming no other channel connection issues exist (see knowledge base article 1008551 (*vCSHB-Ref-992) - Troubleshooting VMware vCenter Server Channel Drops*), you can increase the amount of disk space allotted to the queues. The default setting is 1GB, which can be insufficient on servers with a large volume of replication traffic and limited VMware Channel bandwidth. If you have sufficient disk space, set the queue size to zero (unlimited) so vCenter Server Heartbeat can use any free disk space to store the queues.

[L9]Exceeded the Maximum Disk Usage on the PASSIVE Server

This message indicates that you have exceeded the amount of allocated disk space reserved for the passive server (safe) queue.

Symptom

Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from the passive server.

Causes

Two of the most common causes are shown below:

- The bottleneck lies between the VMware Channel NIC and the disk subsystem on the passive server. Replication traffic passes across the VMware Channel faster than it can be written to disk on the passive server. The excess is buffered temporarily in the passive server (safe) queue. The size of the queue can eventually exceed the allotted disk quota.
- If the passive server is much less powerful than the active server in terms of processor speed, RAM, or disk performance, it can lag behind the active server during periods of high replication activity. Monitor one or more Windows performance counters to determine the component experiencing sustained high activity. Intensive page file use or persistently large disk queue length can indicate a problem. Upgrade one or more physical components of the server.

Either server can be active or passive. If the Secondary server is more powerful than the Primary server, hardware-related issues can only occur while the Secondary server is in the active role.

Resolution

To resolve this issue:

- If you have multiple physical disks on each server, locate the vCenter Server Heartbeat active and passive server queues on a separate physical disk, away from the Windows directory, the Windows page file, and any protected files help to alleviate disk performance issues:

  a Shut down vCenter Server Heartbeat.

  b Open the **Server Configuration** wizard and click the **Logs** tab.

  c Set the path for **Message Queue Logs Location** and click **Finish**.

  d Start vCenter Server Heartbeat on both servers.

  The selected path is applied to all vCenter Server Heartbeat queues on both servers.

- Increase the amount of disk space allotted to the queues. However, if a hardware issue is the root of the problem, correct that problem at the source.
- The size of the passive server queue can increase sharply in response to certain types of file write activity on the active server, such as when vCenter Server Heartbeat is replicating a large number of very small updates of a few bytes each. The volume of update traffic can be far greater than the physical size of the files on the disk, and the passive server queue can become disproportionately large. You can see this pattern of disk activity during the population of Full-Text Catalogs in Microsoft SQL Server. Increase the amount of disk space available for the queues. Move the queues to their own physical disk, upgrade the memory or the disk subsystem.
- vCenter Server Heartbeat requires a certain amount of system resource for its own basic operations and requires some additional resources for processing replication traffic. This is in addition to the resources used by Windows and other applications running on the server, including critical applications protected by Heartbeat. Allocate sufficient resources for all the applications and services running on such a server to provide maximum performance, stability, and resilience for changing client, server, and network activity.

[L20]Out of Disk Space (VCChannelOutOfDiskSpaceException)

This message indicates that one of the servers in the pair has run out of disk space without reaching its preset quota.

Symptom

Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from either server in the pair.

Cause

One of the queues has exceeded the amount of physical disk space available for it without reaching its quota limit. For example, if the maximum queue size is set to 5GB, but only 3GB of physical disk space remains, this error message is reported if one of the queues exceeds 3GB in size.

Resolution

Free up more disk space or move the queues to a disk with sufficient free space to accommodate queue sizes up to the limit configured for Maximum Disk Usage.

Application Slowdown

Operations performed by the application can take longer to complete, and in turn, can affect the time required to log in to a remote client, or to open or save a file. This is true for both servers running vCenter Server Heartbeat and for servers running any other application. vCenter Server Heartbeat can monitor system performance counters and display warnings when predefined thresholds are exceeded, but it does not actively manage system resources for other applications. Like any other application, it also requires a finite amount of resources for its own operations in addition to the resources used by the operating system and the protected application.

The machines hosting vCenter Server Heartbeat must meet recommended hardware requirements and must be powerful enough to support the load, the protected applications, and any other critical applications running on the same server pair.

Poor Application Performance

When applications are competing for resources, one or more applications can perform poorly.

Symptom

Neither server in the pair can accommodate the load placed upon it during normal operation.

Cause

The Primary server's resource usage in one or more areas reached close to the maximum before vCenter Server Heartbeat was installed.

Resolution

Heartbeat Diagnostics can report these conditions and issues warnings if CPU usage or memory usage exceed a certain percentage of the available resource. Information provided by Heartbeat Diagnostics can minimize the risk of application slowdown by identifying needed hardware upgrades on the Primary server.

Both Servers Can Accommodate the Initial Load but the Load Has Increased

Any software installed on a server or workstation consumes a finite amount of system resources when it runs and it must share the resources it uses with any other applications running at the same time. Increased demand caused by additional user activity can have an impact on the server performance.

Symptom

Increased user activity slows application response time.

Causes

The server pair operates normally when vCenter Server Heartbeat is first installed, but performance decreases due to increased user activity. For example, users on the SQL Server system increase or the typical usage pattern becomes more intense. This can be a gradual and sustained increase over time, or transient if a specific event triggers a temporary surge in user activity.

Resolution

If the situation is sporadic, it can correct itself when the load decreases. If the increase is sustained and permanent, upgrade the server hardware.

One Server Can Provide Adequate Resource Support, but the Other Cannot

If the total resource requirements of the applications exceed the available physical resources, the operating system attempts to provide resources, but leaves some applications under resourced. When this situation occurs, an application cannot obtain enough memory to operate normally, or a process must wait before accessing the hard disk

Symptom

Applications operate normally when the Primary server is active but operate slowly when the Secondary server is active (or the reverse).

Cause

A large discrepancy occurs in the processing power between the Primary and Secondary servers. One server can handle the operational load while the other cannot. The load on a server is greater while in the active role when the protected application starts. Applications on the server pair run successfully when the Primary server is active, but experience performance issues when the Secondary is active (or the reverse). Problems can arise even when the more powerful server is active.

Resolution

Both servers must have approximately equivalent processing power, RAM and disk performance. Upgrade the hardware on one server in the pair so that the two servers have roughly the same performance.

Scheduled Resource Intensive Tasks

Scheduling multiple resource intensive tasks at the same time can adversely impact server performance and affect application performance.

Symptom

Resource-intense scheduled tasks impact performance at certain times.

Cause

Two or more resource-intense processes run simultaneously or one process performs actions that increase the load on vCenter Server Heartbeat by triggering additional and sometimes unnecessary replication traffic. Examples: processes such as backups, database maintenance tasks, disk defragmentation, or scheduled virus scans.

Resolution

Schedule operations so that they do not overlap and schedule them outside regular working hours, when fewer users are accessing the protected application and consequently less load on the server.

Appendix – Setup Error Messages

Table A-1. Setup Error Messages

Message	Pri	Sec	Level	Test
10 – 'The pre install check data file does not have the correct format. Setup cannot continue'.	No	Yes	Critical Stop	Check that the file adheres to the correct formatting and structure for use in analysis on the Secondary.
Setup has detected incompatible versions of the collector version $x and the analyzer version $y dll. This would suggest different versions of Setup have been run on the Primary and Secondary servers.	No	Yes	Critical Stop	Check that the analyzer and collector dlls are compatible.
File $x cannot be analyzed it may be corrupt Setup is unable to continue. If the file has been opened check that it has not been saved with Word Wrap.	-	Yes	Critical Stop	Check file format is correct.
190 – This server is a #1# domain controller. vCenter Server Heartbeat must not be installed on a domain controller.	Yes	Yes	Critical Stop	Test whether the server is a domain controller.
173 – vCenter Server Heartbeat does not support the '/3GB' switch on Windows 2000 Standard Edition.	Yes	Yes	Critical Stop	Test for /3GB on Windows 2000
175 – vCenter Server Heartbeat requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.	Yes	Yes	Critical Stop	
103 - vCenter Server Heartbeat does not support #1#. The following are supported Windows 2000 Server SP4 or greater; Windows Server 2003 SP1 or greater.	Yes	Yes	Warning	
200 - Your #1# server uses the Intel ICH7 chipset and Windows 2000 has been detected. This combination is incompatible with vCenter Server Heartbeat.	Yes	Yes	Critical Stop	
217 - vCenter Server Heartbeat is not supported on Windows Storage Server Edition.	Yes	Yes	Warning	
106 - Primary and Secondary OS versions are not identical, #1# vs. #2#: and require the same Service Pack level.	-	Yes	Critical Stop	Compatibility check on secondary.
208 - You are running a 64-bit version of Windows on one of your servers and a 32-bit version of Windows on the other. This is not supported.	-	Yes	Critical Stop	Compatibility check on secondary.
111 - The system folders on primary and secondary system must be the same. Setup has detected that the secondary system folder is #2# and the primary was #1#.	-	Yes	Critical Stop	Compatibility check on secondary.

Table A-1. Setup Error Messages (Continued)

Message	Pri	Sec	Level	Test
113 - You do not have enough total memory to install vCenter Server Heartbeat on your #1# server. You must have at least 1GB.	Yes	Yes	Critical Stop	
VMware recommend a minimum of 2GB. Note actual memory requirements depend on the application load; and may require more memory.	Yes	Yes	Warning	
117 - You do not have enough free disk space to install vCenter Server Heartbeat. You must have at least 2GB available.	Yes	Yes	Critical Stop	
118 - For every volume on the primary system that contains protected data a corresponding volume must exist on the secondary server. In most cases this means that for every volume on the primary server a volume with the same drive letter (such as D:\) must exist on the secondary server. If this is not the case, the secondary server must be modified to meet this requirement.	-	Yes	Warning	Compatibility check on secondary.
204 - Your operating system on your #1# server is #2# and you are running with a Windows 2000 driver for your NC77xx NIC(s). In order to prevent system crashes you must upgrade to a Windows 2003 driver; the name for those drivers ends with '57XP32.sys' and not with '57W2K.sys'	Yes	Yes	Critical Stop	
212 - The number of Free System Page Table Entries on this server has dropped to #1#. This is too low. You should have at least #2# Free System Page Table Entries available.	Yes	Yes	Critical Stop	
201 - #1#: This service is incompatible with running vCenter Server Heartbeat and must be stopped before vCenter Server Heartbeat can be installed.	Yes	Yes	Warning	
209 - Double-Take drivers have been detected on this server. To avoid compatibility problems please uninstall Double-Take before re-running setup.	Yes	Yes	Critical Stop	
Oracle has been detected on this Server. vCenter Server Heartbeat does not support Oracle on the same server as VirtualCenter.	Yes	Yes	Critical Stop	It is recommended that you move Oracle to another server before attempting to re-run Setup, OR that you move VirtualCenter to another server and deploy vCenter Server Heartbeat there.

Glossary

A

Active
The functional state or role of a server visible through the network by clients running protected applications and servicing client requests.

Alert
A notification sent to a user or entered into the system log indicating an exceeded threshold.

Active Directory (AD)
Presents applications with a single, simplified set of interfaces so users can locate and use directory resources from a variety of networks while bypassing differences among proprietary services. vCenter Server Heartbeat switchovers and failovers require no changes to AD, resulting in switchover and failover times measured in seconds.

Active – Passive
The coupling of two servers: one server visible to clients on a network and providing application service, the other server not visible and not providing application service.

Active Server Queue
The staging area of the active server used to store intercepted data changes before being transported across the VMware Channel to the passive server.

Advanced Configuration and Power Interface (ACPI)
A specification that dictates how the operating system can interact with hardware using power saving schemes. Primary and Secondary servers must have the same ACPI compliance.

Asynchronous
A process whereby replicated data is applied (written) to the passive server independently of the active server.

B

Basic Input/Output System (BIOS)
The program a personal computer's microprocessor uses to start the computer system after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

C

Cached Credentials
Locally stored security access credentials used to log in to a computer system when a Domain Controller is not available.

Channel Drop
An event in which the dedicated communications link between the Primary and Secondary server fails, often resulting in the passive server becoming active and consequently creating a split-brain syndrome.

Channel NIC (Network Interface Card)
A dedicated subnet used by the VMware Channel.

Cloned Servers
Two servers in a pair with the same configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of vCenter Server Heartbeat.

Cloning Process
The vCenter Server Heartbeat process whereby all installed applications, configuration settings, the machine name, security identifier (SID), and IP address are copied to a second server.

Crossover Cable
A network cable that crosses transmit and receive lines.

D

Data Replication
The transmission of protected data changes (files and registry) from the active to the passive server through the VMware Channel.

Device Drivers
A program that controls a hardware device, linking it to the operating system.

Disaster Recovery (DR)
A term indicating how you maintain and recover data in light of a disaster such as a hurricane or fire. vCenter Server Heartbeat achieves DR protection by placing the Secondary server at on offsite facility and replicating the data through a WAN link.

DNS (Domain Name System) Server
Responsible for providing a centralized resource for clients to resolve NetBIOS names to IP addresses.

Domain
A logical group of client server based machines where the administration rights across the network are maintained in a centralized resource called a domain controller.

Domain Controller (DC)
The server responsible for maintaining privileges to domain resources, sometimes called AD controller in Windows 2000 and above domains.

F

Failover
The process by which the passive server assumes the active role when it no longer detects that the active server is alive as a result of a critical unexpected outage or server crash.

Full System Check (FSC)
The internal process programmatically started at the initial connection of a server pair or manually triggered through the vCenter Server Heartbeat Console. The FSC verifies the files and registry keys, and synchronizes the differences.

Fully Qualified Domain Name (FQDN)
Also known as an absolute domain name, a FQDN specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. Example: `somehost.example.com.`, where the trailing dot indicates the root domain.

G

Graceful (Clean) Shutdown
vCenter Server Heartbeat shuts down with no data loss after completing replication using the vCenter Server Heartbeat Console.

H

Hardware Agnostic
A key vCenter Server Heartbeat feature enabling the use of servers from different manufacturers, models, and processing power in a single vCenter Server Heartbeat server pair.

Heartbeat
The packet of information issued by the passive server across the VMware Channel, which the active server responds to, indicating its presence.

Heartbeat Diagnostics
The umbrella name for the VMware process and tools used to check the production server health and applicability to the implementation of the vCenter Server Heartbeat solution.

High Availability (HA)
Keeping users seamlessly connected to their applications, regardless of the nature of a failure. LAN environments are ideally suited for HA.

Hotfix
A single, cumulative package that includes one or more files used to address a problem in a product.

I

Identity
The reference of a server's position in the server pair based upon hardware, either the Primary server or the Secondary server.

L

Low Bandwidth Module (LBM)
A vCenter Server Heartbeat Module that compresses and optimizes data replicated between a Primary and Secondary server, thereby delivering maximum data throughput and improving application response time on congested WAN links.

M

Machine Name
The Windows or NETBIOS name of a computer.

Management IP Address
An additionally assigned unfiltered IP address used for server management purposes only.

Many-to-One
One physical Secondary server (hosting more than one virtual server) can provide protection to multiple physical Primary servers.

N

Network Monitoring
Monitoring the active server's capability to communicate with the rest of the network by polling defined nodes around the network at regular intervals.

P

Passive
The functional state or role of a server that is not delivering service to clients and is hidden from the rest of the network.

Passive Server Queue
The staging area on the passive server used to store changes received from the active server before they are applied to the passive server's disk or registry.

Pathping
A route-tracing tool that sends packets to each router on the way to a final destination and displays the results of each hop.

Plug and Play (PnP)
A standard for peripheral expansion on a PC. When starting the computer, Plug and Play (PnP) configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in
An optional module that can be installed into a vCenter Server Heartbeat server to provide additional protection for a specific application.

Pre-Installation Checks
A list of system and environmental checks performed before the installation of vCenter Server Heartbeat.

Principal IP address
An IP address used by clients to contact the server through drive mappings, UNC paths, DNS resolved paths, to access the server's services and resources.

Principal NIC
The network card that hosts the Principal IP address.

Protected Application
An application protected by vCenter Server Heartbeat.

Q

Quality of Service (QoS)
An effort to provide different prioritization levels for different types of traffic over a network. For example, vCenter Server Heartbeat data replication can have a greater priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

R

Remote Desktop Protocol (RDP)
This multi-channel protocol connects to a computer running Microsoft Terminal Services.

Replication
The generic term given to the process of intercepting changes to data files and registry keys, transporting the changed data across the VMware Channel, and applying them to the passive server so both servers are maintained in a synchronized state.

Role
The functional state of the server in the pair that can be either active or passive.

Rule
A set of actions vCenter Server Heartbeat to perform when defined conditions are met.

S

Security Identifier (SID)
A unique alphanumeric character string that identifies each operating system and each user in a network of Windows NT, Windows Server 2000, Windows Server 2003, and Windows Server 2008 systems.

Server Monitoring
Monitoring the active server by the passive server, using a heartbeat message, to ensure that the active server is functional.

Server Pair
The generic term used to describe the coupling of the Primary and Secondary server in vCenter Server Heartbeat.

Shared Nothing
A key vCenter Server Heartbeat feature whereby hardware is not shared between the Primary and Secondary servers, thus preventing a single point of failure.

SMTP
A TCP/IP protocol used in sending and receiving e-mail between or among servers.

Split-brain Avoidance
A unique feature of vCenter Server Heartbeat that uses various checks to overcome a scenario where both Primary and Secondary servers attempt to become active at the same time, leading to an active-active rather than an active-passive model.

Split-brain Syndrome
A situation where both the Primary and Secondary servers in a vCenter Server Heartbeat server pair are operating in the active mode and attempting to service clients, causing different data updates to be applied independently to each server.

Subnet
A division of a network into an interconnected but independent segment or domain, to improve performance and security.

Storage Area Network (SAN)
A high-speed special-purpose network or (sub-network) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

Switchover
The graceful transfer of control and application service to the passive server.

Synchronize
The internal process of transporting 64KB blocks of changed files or registry key data, through the VMware Channel from the active server to the passive server. The data on the passive server is a mirror image of the protected data on the active server, a required condition for data replication on a vCenter Server Heartbeat server pair.

System State
Data that comprises the registry, COM+ Class Registration database, files under Windows File Protection, and system boot file. Other data can be included in the system state data.

T

Task
An action performed by vCenter Server Heartbeat when defined conditions are met.

Time-To-Live (TTL)
The length of time that a locally cached DNS resolution is valid. The DNS server must be re-queried after the TTL expires.

Traceroute
A utility that records the route through the Internet between the computer and a specified destination computer.

U

Ungraceful (Unclean) Shutdown
A shutdown of vCenter Server Heartbeat resulting from a critical failure or by shutting down Windows without first performing a proper shutdown of vCenter Server Heartbeat, resulting in possible data loss.

Unprotected Application
An application that is not monitored or its data replicated by vCenter Server Heartbeat.

V

VMware Channel
The IP communications link used by vCenter Server Heartbeat for heartbeat and replication traffic.

VMware vCenter Server Heartbeat
The core replication and system monitoring component.

VMware vCenter Server Heartbeat Packet Filter
The network component installed on both servers that controls network visibility.

VMware vCenter Server Heartbeat Switchover and Failover Process

A vCenter Server Heartbeat unique process whereby the passive server gracefully (Switchover) or unexpectedly (Failover) assumes the role of the active server providing application services to connected clients.

Virtual Private Network (VPN)

A private data network that uses the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VMware Web Site

The VMware web site dedicated to support partners and customers providing technical information, software updates, and license key generation.

W

Windows Management Instrumentation (WMI)

A management technology using scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, and groups.